

Version

3.1

TNT SOFTWARE

ELM Performance Manager™

Administrator's Guide

TNT SOFTWARE

ELM Performance Manager 3.1 Administrator's Guide



Copyright © 1997-2003 TNT Software
All Rights Reserved
2001 Main Street
Vancouver, WA 98660 USA
Phone 360.546.0878 • Fax 360.546.5017
<http://www.tntsoftware.com>
support@tntsoftware.com

Table of Contents

ELM Performance Manager 3.1 Terminology.....	1
Installation of ELM Server and ELM Console	4
Installing the ELM Console.....	6
Agents	7
Installing Service Agents.....	7
Installing Service Agents Using Setup Package	9
Installing Remote Agents	10
Troubleshooting Service Agent Installation	11
Troubleshooting Service Agent Communications.....	12
Monitor Items	13
Monitor Item Best Practices	14
Creating Monitor Items	14
ELM Server Monitor.....	14
How To Create an ELM Server Monitor	15
Performance Alarms	16
How To Create a Performance Alarm	16
Performance Collector.....	17
How To Use Performance Collectors	17
Process Monitor	18
How To Create a Process Monitor.....	19
WMI Monitor	20
How To Create a WMI Monitor.....	20
Monitor Item Actions	21
Event Filters, Rules and Notification Methods	23
Event Filters.....	23
Notification Methods	24
Alerts.....	26
How To Create an Alert	26
Beeps	27
How To Create a Beep Notification Method	27

Command Script	28
How To Create a Command Script Notification Method.....	28
How To Programmatically Enable or Disable Items	29
Forward Event	31
How To Forward an Event.....	31
Instant Message	31
How To Use an Instant Message Notification Method	31
Mail Notification.....	31
How To Use MAPI Notification.....	31
How To Create an SMTP Notification Method	31
Marquee Device	31
How To Create a Marquee Notification Method.....	31
Network Message Settings	31
How To Create a Network Popup Notification Method.....	31
Pagers	31
How To Create a Pager Notification Method.....	31
SNMP Notification	31
How To Create an SNMP Notification Method.....	31
How To Create an SNMP Trap Notification Method.....	31
Sound File	31
How To Create a Sound File Notification Method	31
Syslog Notification	31
How To Create a Syslog Notification Method	31
Text-To-Speech Notification.....	31
How To Create a Text-to-Speech Notification Method	31
Web Post Notification.....	31
How To Create a Web Post Notification Method.....	31
Rules.....	31
How To Create a Rule	31
Reports.....	31
How To Create Reports	31
How To Schedule Reports.....	31
How To Add a Chart to a Report	31
Web Viewer	31
Web Viewer Security	31
Web Viewer User Interface	31
Pre-Configured Items	31

ELM Performance Manager 3.1

Terminology

The following terms are used in this document, in the ELM Performance Manager product documentation (EPMMC.CHM) and in ELM Performance Manager.

Term	Description
ELM Server	The ELM server process (epmsvr.exe) and supporting modules (DLLs). This component is comprised of several engines that handle such tasks as creating and maintaining a database for data storage, archiving and reporting, managing Agents and Agent licensing, processing Event Filters and Rules, and executing Notification Methods.
ELM Server Database	The ELM Server database contains data collected from Agents (performance data) and Alerts generated by Actions and the Alert Notification Method. The ELM Server can use Microsoft Access (runtime included), Microsoft SQL Server 6.5 or later, Microsoft SQL Desktop Engine (MSDE), or Oracle 8i or later as its database platform. The ELM Server database requires the MDAC 2.6 SP1 or later and JET 4.0 SP3 or later.
ELM Console	The ELM Console refers to the snap-in that resides in a Microsoft Management Console. The ELM Console is the primary user interface for the product. The ELM Console is freely distributable throughout your organization. Installing the ELM Console requires MMC 1.2 or later; you can save the ELM Console in MMC 2.0 format when running on Windows XP or Windows 2003. Each snap-in can connect to multiple ELM Servers, and the ELM Console snap-in can be co-mingled with other MMC snap-ins to provide single-seat administration.
Web Viewer	The Web Viewer is an HTTP/XML-based interface to ELM Server Objects. It is a set of COM objects within a set of Active Server Pages that runs under Internet Information Services 5.0 and later. The server side of the Web Viewer is installed using the setup package for ELM. The client side of the Web Viewer is any Javascript/XML-capable Web browser. The latest versions of Netscape and Internet Explorer support both Javascript and XML and will provide the richest Web Viewer experience. Because the client side is simply a Web browser, most organizations will not have to deploy any software to client machines in order to utilize the Web Viewer.
ELM Server Objects	

Term	Description
Agent	A system monitored by an ELM Server, or a system that transmits messages to an ELM Server. There are three types of Agents: Service Agents, Remote Agents and Remote IP Agents.
Service Agent	The Service Agent process (tntagent.exe) and supporting modules. This component executes Monitor Items, collects data, transmits collected data to the ELM Server, and executes the configured Actions for assigned Monitor Items. Service Agents run as a service on the monitored Agent. Service Agents are required in order to monitor health and performance and other subsystems in real-time. Service Agents can only be run on Windows NT, Windows 2000, Windows XP and Windows 2003 computers.
Remote Agent	Remote Agents are also called <i>Agentless</i> because, unlike a Service Agent, nothing is installed on the system being monitored. Remote Agents are Windows workstations and servers. The actual monitoring functions for a Remote Agent execute within the ELM Server Process. As a result, Remote Agents cannot be monitored in real-time. In addition, Remote Agents add overhead to the ELM Server process (~10MB per Remote Agent, depending on what Monitor Items are used).
Alert	A special type of event that can be generated from a Monitor Item or by the Alert Notification Method. Alerts are stored in the TNTAlerts database and displayed in the Alerts container within the ELM Console. By design, all entries in the TNTAlerts database are displayed in the Alerts container. Alerts have two Status settings: Open and Closed. You can configure the ELM Console to display Alerts based on its status (Open, Closed, or Both). You can also re-open Alerts that have been closed.
Event Filters	Event Filters are displayed within the Event Filter container within the ELM Console. Event Filters are used to process incoming Alerts to determine whether or not the Alert should cause a Rule to execute a Notification Method. Event Filters can be used to isolate a single Alert or specific set of Alerts, or to isolate all except for a single Alert or specific set of Alerts. You can create an unlimited number of Event Filters.
Monitor Item	A Monitor Item is the individual thing being monitored. Monitor Items are displayed within the Monitor Item container in the ELM Console. Monitor Items watch for conditions and thresholds, collect data, check Agent, system and application availability and verify quality of service.
Notification Methods	Notification Methods are used to notify administrators/end-users or take corrective action. Notification Methods are displayed within the Notification Method container of the ELM Console. The ELM Server has a rich notification engine that can execute a variety of Notification Methods. You can use beeps and sounds, electronic mail, numeric and alphanumeric pagers, SNMP traps, Syslog messages and scripts as Notification Methods.
Performance Data	Performance Data refers to the Performance Objects and Performance Object Counters that are displayed in the Performance Data container within the ELM Console. Performance Objects are published by the operating system, software applications and hardware devices. Performance Counters can be monitored for thresholds and collected for capacity planning purposes. You can also import performance counters for

	monitoring and collection from any Windows NT, Windows 2000, Windows 2003, or Windows XP computer.								
Reports	Reports refer to report objects that perform database queries and return the results in a pre-designed format. The ELM Server includes a report engine that enables administrators/end-users to create reports without requiring any additional software. Reports are displayed in the Reports container within the ELM Console. Reports can be generated both on an ad hoc basis and at periodic intervals, and output to a variety of formats.								
Rules	Rules link Event Filters with Notification Methods. When one or more Event Filters assigned to a Rule are matched, the Notification Method(s) assigned to the Rule is/are executed. Rules are displayed in the Rules container within the ELM Console. Each Rule can have multiple Event Filters assigned to it, and each Rule can trigger multiple Notification Methods.								
Other Terms									
	<table> <tr> <th>Term</th><th>Description</th></tr> <tr> <td>Actions</td><td> Actions are a form of notification that is executed by a Monitor Item. As a result, Actions occur outside of the ELM Server's notification engine. There are four Actions that can be executed: generate Alert, generate application event log entry, send a Network Pop-up Message or execute a script. </td></tr> <tr> <td>Quality of Service (QoS)</td><td> Quality of Service deals with response times. It is a level of monitoring above general availability. Determining that a critical service or application is available is only one part of proactive monitoring. Ideally, you should also monitor the responsiveness or quality of service of your critical business applications. </td></tr> <tr> <td>Wizards</td><td> Creating new objects in ELM is accomplished through the use of Wizards. Each Wizard takes the administrator/end-user step-by-step through the creation of an object. Wizards are used to reduce the learning curve for ELM and increase usability. Wizards are launched whenever new object creation is invoked from within the ELM Console. At the end of each Wizard is an option to re-run the Wizard to create additional objects, making multiple object creation quick and easy. </td></tr> </table>	Term	Description	Actions	Actions are a form of notification that is executed by a Monitor Item. As a result, Actions occur outside of the ELM Server's notification engine. There are four Actions that can be executed: generate Alert, generate application event log entry, send a Network Pop-up Message or execute a script.	Quality of Service (QoS)	Quality of Service deals with response times. It is a level of monitoring above general availability. Determining that a critical service or application is available is only one part of proactive monitoring. Ideally, you should also monitor the responsiveness or quality of service of your critical business applications.	Wizards	Creating new objects in ELM is accomplished through the use of Wizards. Each Wizard takes the administrator/end-user step-by-step through the creation of an object. Wizards are used to reduce the learning curve for ELM and increase usability. Wizards are launched whenever new object creation is invoked from within the ELM Console. At the end of each Wizard is an option to re-run the Wizard to create additional objects, making multiple object creation quick and easy.
Term	Description								
Actions	Actions are a form of notification that is executed by a Monitor Item. As a result, Actions occur outside of the ELM Server's notification engine. There are four Actions that can be executed: generate Alert, generate application event log entry, send a Network Pop-up Message or execute a script.								
Quality of Service (QoS)	Quality of Service deals with response times. It is a level of monitoring above general availability. Determining that a critical service or application is available is only one part of proactive monitoring. Ideally, you should also monitor the responsiveness or quality of service of your critical business applications.								
Wizards	Creating new objects in ELM is accomplished through the use of Wizards. Each Wizard takes the administrator/end-user step-by-step through the creation of an object. Wizards are used to reduce the learning curve for ELM and increase usability. Wizards are launched whenever new object creation is invoked from within the ELM Console. At the end of each Wizard is an option to re-run the Wizard to create additional objects, making multiple object creation quick and easy.								

Installation of ELM Server and ELM Console

Installing the **ELM Server** is a relatively easy and straightforward process. Once you've determined that your system meets the minimum system requirements, you can begin your installation by performing the actual installation of the application.

ELM is distributed electronically from TNT Software's Web site (<http://www.tntsoftware.com>). It is packaged into a self-extracting executable that will launch the setup process when executed:

Windows 2003, Windows 2000 and Windows XP, as well as Windows NT computers with the Windows Installer service installed can use the Microsoft Installer package (MSI package). Windows NT computers without the Windows Installer service require the EXE package. You can download the Windows Installer for both NT 4.0 and Windows 2000 from [Microsoft](http://www.microsoft.com).

During Setup, the following services (and any services dependent on the following services) will be stopped and restarted:

- IIS Admin Service
- SNMP Service
- SNMP Trap Service
- ELM Server service (if upgrading only)
- TNT Agent service (if upgrading only)

» To Install the ELM Server:

1. Double-click the MSI or EXE file you downloaded to execute it. The Setup Wizard will launch.
2. Click Next to continue. The License Agreement screen will appear.
3. Select I accept the license agreement and click Next to continue. The ReadMe Information screen will appear.
4. Read the contents of the ReadMe file and click Next to continue. The Select Features screen will appear.
5. Select the feature(s) you want to install. When selecting the Server or Console components, you can use the Browse button to choose the destination folder. Use the Disk Cost button to check available disk space. Click Next to continue. The User Information screen will appear.
6. Enter the Company Name and Serial Number as it appears on your SLA. If this is an evaluation version, enter the Company Name and leave the Serial Number field set to Evaluation. Select the option that says Anyone who uses this computer and click Next to continue. If this is an evaluation version, the expiration date will be displayed when you click Next. If this is a non-eval version, a confirmation dialog will appear when you click Next.

7. Click Next to continue, and click OK to clear the dialog message that appears. The Service Account Logon screen will be displayed.
8. In the Username field, enter the account you want to use for the service account. This account must have administrative rights on the ELM Server and on all Windows-based Remote Agents. Enter the password for this account in the Password field.
9. Click Next to continue. If the account specified in the preceding step does not already have Log on as a Service rights on the ELM Server, the Setup process will grant this right to the account.
10. If IIS is installed, the Web Site Name screen will appear. If you wish to install the Web Viewer component, leave the Create the ELM Web Site virtual directory on this computer checkbox checked. Leave the default Alias set to EEM31. Select the Default Web Site and click Next to continue. Note: if you do not create the Web Viewer virtual directory during the initial install of ELM, you will need to create the virtual directory manually.
11. The Ready to Install the Application screen will appear.
12. Click Next to continue. Setup will copy the files to the target destination, register its components, install the ELM Server service and launch the Agent Installation Wizard.
13. Click Next to continue. Note: If you are presented with the Upgrade Previous Version dialog box instead of the Agent Installation Wizard, clear all of the checkboxes on this dialog box and click Next to continue. Once the file copy process has completed, the Database Connection Wizard will launch.
14. Click Next to proceed past the Wizard's Welcome screen. The Database Type screen will appear. Using the Database Type dropdown, select the type of database you want to use.
15. Click Next to continue. The next screen depends on what database type you selected:
 - If you select Microsoft Access, the Microsoft Access screen will appear. Select the path and filename for the Access database you want created. By default, a database called ELM.MDB will be created in the ELM Server directory. To accept this default, click Next. To change the database name or location, enter the path and filename you want to use, or use the Browse button to browse for the path. Click Next to continue.
 - If you select Microsoft SQL Server, the Microsoft SQL Server screen will appear. Enter the Computer Name of the SQL Server, the database name and the username and password for an account that has database owner (dbo) rights on the SQL Server database you created. You should also use this option when using Microsoft SQL Server Desktop Engine (MSDE) as your database platform. Click Next to continue.
 - If you select Oracle, the Oracle Database screen will appear. Enter the name of the System DSN you created. Enter the username and password for an account that has database owner (dbo) rights on the Oracle database you created. Click Next to continue.
16. Click Finish to complete the Database Connection Wizard.
17. Click Finish to complete Setup.

Installing the ELM Console

Installing the **ELM Console** is a relatively easy and straightforward process. Once you've determined that your system meets the minimum requirements for installation, you can begin your installation by performing the actual installation of the application.

» To Install the ELM Console:

1. Double-click the file you downloaded to execute it. The Setup Wizard will launch.
2. Click Next to continue. The License Agreement screen will appear.
3. Select I accept the license agreement and click Next to continue. The ReadMe Information screen will appear.
4. Read the contents of the ReadMe file and click Next to continue. The Select Features screen will appear.
5. Select the Server component and choose Entire feature will be unavailable. Make sure just the Console component is selected.
6. Click Next to begin the install process.
7. Click Finish to complete the install process.

Agents

Creating and managing Agent Objects

Agent is the general term used to describe a managed system. There are three classes of Agents:

- Cluster Agent – for Windows NT, Windows 2000 and Windows 2003 clusters
- Server Agent – for Windows NT, Windows 2000 and Windows 2003 Servers
- Workstation Agent – for Windows NT Workstation, Windows 2000 Professional and Windows XP Professional

With respect to Cluster, Server and Workstation Agents, there are two types:

- Service Agents – code that runs as a service on the monitored system
- Remote Agents – Agentless monitoring, where the ELM Server performs monitoring/collection.

Installing Service Agents

Service Agents and ELM Servers can have one-to-one or one-to-many relationships. An ELM Server can monitor multiple Service Agents and a Service Agent can be monitored by multiple ELM Servers. Each Service Agent maintains separate configuration, collection set and cache files for each Server that is monitoring it.

The Service Agent is comprised of a 32-bit, multithreaded executable called TNTAGENT.EXE, its companion DLLs and its configuration data (TNTAgent.dat). These files exist in the %systemroot%\TNTAgent on the monitored system. The Service Agent can run in the security context of the LocalSystem, or in a user security context (e.g., using a *service account*).

Service Agents typically consume about 7-15MB of physical memory, and less than .1% of the overall CPU time on the monitored system. The amount of resources actually consumed depend on the number of Monitor Items applied to the Agent, the frequency at which those Monitor Items are executed, and the amount of data generated by or being collected from the monitored system.

You can use the ELM Console to install Service Agents remotely, or you can install them manually on the target machine. Service Agents are only used for monitoring Windows NT, Windows 2000, Windows 2003, and Windows XP systems; if you are monitoring a computer with an Alpha or RISC processor, or if you do not wish to install software on the monitored system, you can use a **Remote Agent**.

» To install a Service Agent:

1. Right-click on the Agents container in the ELM Console and select **All Tasks | New Agent**. The Agent Installation Wizard will launch. If the Welcome dialog is displayed, click **Next** to continue.
2. From the dropdown, select **Service Agent** and click **Next** to continue.
3. Enter the **host name**, **fully-qualified domain name**, or **IP address** of the system you want to monitor. Click the **Browse** button to browse your network if you are unsure of the computer's name. Click **Next** to continue.
4. The **Logon Account** dialog will appear. You can run a Service Agent under a user account, or under the LocalSystem account. Enter the account information and click **Next** to continue.
5. In the **Listen on TCP Port** field, enter the TCP port on which you want the Agent to listen. Service Agents communicate with the ELM Server over TCP/IP sockets. By default, Service Agents listen on TCP port 1253. You can change the port used by the Agent by selecting an alternative TCP port. Use the **Test** button to verify that the port is available.

 Note

Once an Agent has been configured to listen on a specific port, you cannot change the port. If you want the Agent to listen on a different port, you will need to remove and re-add the Agent using the new port.

6. Click **Next** to continue. The copy file process will begin. The Agent executable, companion DLL files and configuration data will be copied to the target computer.



Important

In order to install a Service Agent, you must have administrative rights on the monitored system. ELM will attempt to install the Service Agent using your current credentials (e.g., the account you're logged on with); if this account does not have administrative rights on the Service Agent, you will be prompted to specify alternate credentials to perform the installation. Another alternative is to use the setup package you downloaded to install the Service Agent.

7. The **Description** dialog will appear. Enter an optional description for this Service Agent, and click **Next** to continue.
8. The **Agent Categories** dialog will appear. Modify the **Categories** field as desired, or leave the default entries. Click **Next** to continue.
9. The **Select Monitors** dialog will appear. Select the Monitor Items you want applied to this Service Agent. Click **Next** to continue. Click **Finish**.
10. Click **OK** to acknowledge the Agent installation. When prompted to install another Service Agent, click **Yes** or **No**, depending on your needs.

Installing Service Agents Using Setup Package

If the Agent you want to monitor is on the other side of a firewall, in a DMZ environment, or located in an environment that restricts the use of NetBIOS and RPC endpoint ports, you can use the Setup package to install an Agent on the remote system and then use the Agent UI to register the Agent with the ELM Server and select monitor items for the Agent.

» To install a Service Agent using Setup:

1. Copy the ELM Setup package to the target computer, and execute the file to begin the install.
2. The Installation Welcome screen will appear. Click **Next** to continue.
3. The License Agreement screen will appear. Read the license agreement and indicate your acceptance of its terms by selecting **I accept the license agreement**. Click **Next** to continue.
4. The ReadMe Information screen will appear. Read the contents of the ReadMe file and click **Next** to continue.
5. The Select Features screen will appear:
 - Click Server and choose **Entire feature will be unavailable**.
 - Click Console and choose **Entire feature will be unavailable**.
 - Click Agent and choose **Will be installed on local hard drive**.
6. Click **Next** to continue, and then **Next** one more time to initiate installation.
7. The Agent executable and support files will be installed. When the installation has completed, the Register Server Wizard will launch.
8. In the **Name** field, enter the host name, IP address or fully-qualified domain name for the ELM Server you want to register. If desired, click the **Browse** button to browse the network for the ELM Server you want to register.
9. In the **Port** field, enter the TCP port on which the ELM Server is listening. By default, ELM Servers listen on the following TCP ports:
 - ELM Enterprise Manager - TCP Port 1251
 - ELM Log Manager - TCP Port 1351
 - ELM Performance Manager - TCP Port 1451

Note

The name field may already be filled in with an Agent name that contains :EEM. The EEM is a visual cue that indicates the product you are running. ELM Performance Manager users will also see the EEM designation and will need to change to the appropriate descriptor (e.g., ELM or EPM).

10. Click **Next** to continue. The Select Monitors dialog box will appear. Put a check in the box to the left of each Monitor Item you want to assign to this Agent. You can view the properties of any Monitor Item by right-clicking the item and selecting **Properties**.
11. Click **Finish** to save the Agent settings and ELM Server registration.

» To Uninstall a Service Agent That Was Installed Using Setup:

1. Open the Control Panel and double-click Add/Remove Programs.
2. Select the product you have installed, either:
 - ELM Enterprise Manager
 - ELM Log Manager
 - ELM Performance Manager
3. Click the Change button.
4. If the Service Agent is the only ELM component installed on this system, or if there are other ELM components (e.g., ELM Server or ELM Console) and you want to uninstall everything, select **Remove** and proceed through the Wizard. If there are other ELM components installed on this system and you do not want to remove them, select **Modify** and continue through the Wizard. When the component dialog is shown, change the Service Agent from **Will be installed on local hard drive** to **Entire feature will be unavailable**. Then, complete the Wizard to remove it.

Installing Remote Agents

You can monitor Windows NT, Windows 2000, Windows XP and Windows 2003 computers without having to install a Service Agent. You can use a Remote Agent. Instead of running a service on the monitored system, the ELM Server collects and monitors the Agent remotely. Because Agent code is not used on the monitored system, this will add overhead to your network and to the ELM Server. However, this scenario is advantageous when you do not want to install any software on the monitored system in order to keep tabs on it. Remote Agents require that the ELM Server service account has administrative privileges on the system being monitored. In addition, Remote Agents require RPC and NetBIOS connectivity between the ELM Server and the monitored system. Because Remote Agents are remotely monitored by the ELM Server, they cannot be monitored in real-time.

» To install a Remote Agent:

1. Right-click on the Agent container in the ELM Console and select **All Tasks | New Agent**. The Agent Installation Wizard will launch. If necessary, click **Next** to continue.
2. From the dropdown, select **Remote Agent** and make sure the **IP Agent** checkbox is not checked. Click **Next** to continue.
3. Enter the **name** or **IP address** of the system you want to monitor. Click the **Browse** button to browse your network if you are unsure of the computer's name. Click **Next** to continue.
4. Modify the **Categories** field as desired, or leave the default entries. Click **Next** to continue.
5. Click **Next** to continue. If there are no monitor items configured, click **Finish** to complete the Wizard. If there are monitor items, the **Select Monitors** dialog will appear. In this event, click on each Monitor Item you want applied to this Service Agent. To create a new Monitor Item, right-click in the white space in this dialog and select **New Monitor Item**. Click **Next** to continue. Click **Finish**.
6. Click **OK** to acknowledge the Agent installation. When prompted to install another Remote Agent, click **No**.

The Remote Agent will be added to the list of monitored systems, and the selected Monitor Items for this Remote Agent will be executed according to their settings.

Troubleshooting Service Agent Installation

Installing a Service Agent is a relatively easy procedure that is usually trouble-free. If you are having problems installing an Agent, some things that you can check are listed below.

- **Does the ADMIN\$ share exist on the Agent machine?** When installing an Agent from the ELM Server, the ELM Server will attempt to connect to the ADMIN\$ share on the Agent machine, so that the Agent executable can be copied to the SYSTEM32 folder on the Agent. If the ADMIN\$ does not exist, re-create it. If this is not an option, follow the procedure for manually installing an Agent, which is detailed below.
- **Do you have good name resolution between the ELM Server and Agent?** Can you ping the Agent by name from the ELM Server? Can you ping the ELM Server by name from the Agent? Are you able to do a NET VIEW on each system from the other system? ELM can use NetBIOS or host name resolution.
- **Are there any firewalls between the ELM Server and this Agent?** Are you able to Telnet from the Agent computer to the appropriate port on the ELM Server? By default, the ELM Performance Manager Server listens on TCP Port 1251.
- Does a **Netstat -a -p tcp** on the ELM Server show it listening on the appropriate port? If you run this command on the Agent, does it show something else listening on port 1253 on the Agent? If the Agent is in a DMZ or a firewall environment, you can use the ELM setup package to install the Agent remotely.
- **Do you have administrative rights on the Agent machine?** Only Administrators can connect to the ADMIN\$ share and install a new service. When you attempt to install an Agent, ELM will first try to use your existing credentials to authenticate you to the Agent machine. If authentication fails, you will be presented with a **Connect As** dialog box, which can be used to specify alternate credentials (e.g., local administrator username and password.) Note: the Connect As dialog box does not support blank passwords. If you do not enter a password, the connection will fail. To get around this limitation, go to a command prompt on the ELM Server machine and make a connection to the IPC\$ share on the Agent machine. You can use the following syntax:

```
net use \\SERVER\IPC$ /user:ABCDE\12345
```

where:

SERVER is the name of the Agent machine

ABCDE is the name of the domain or machine containing the account you're using

12345 is the name of the account with administrative rights

- **Are there any services in a Stop Pending or Start Pending state on the Agent?** This may prevent ELM from installing an Agent service. You can use a command-line utility included with ELM to check this. The utility, SM.EXE is a command line utility that can query the Service Control Manager on a local or remote machine. It's usage is:

Local machine - SM /dis

Remote machine - SM \\SERVER /dis

If you see any Start Pending or Stop Pending services, you will need to get them at a stable state (started or stopped) before you can install the Agent service.

- **Have any special security modifications been made to the Agent system?** These include things like restrictive registry or NTFS permissions, revoking of user rights assignments, and as previously mentioned, the removal of the ADMIN\$ share.

If none of these solutions resolves your issue, please contact TNT Software's [Product Support Group](#) for assistance.

Troubleshooting Service Agent Communications

If an Agent does not send, or does not appear to be sending, data to your ELM Server(s), there are a few things to check to make sure things are installed and configured properly. The easiest path for troubleshooting these situations is to check the basic things first.

- **Is the Agent service running, or is the Agent disabled?** The Agent will only monitor, collect and transmit data when the TNT Agent service is running and the Agent is enabled.
- **Has the Agent been configured to collect data?** From the ELM Server, double-click the Agent that is not sending data, and look at the Monitor Items tab.
- **Do you still have IP connectivity and good name resolution between the ELM Server and Agent?** IP connectivity and healthy name resolution are essential for ELM to operate properly.
- **Have the ELM TCP/IP ports been blocked through a firewall, packet filtering or some other mechanism?** By default, the TNT Agent listens on TCP port 1253, and the ELM Performance Manager Server listens on TCP Port 1451.

Try telnetting to the appropriate ports in each direction:

- From the ELM Server, try to Telnet to port 1253 on the Agent
- From the Agent, try to Telnet to the appropriate port on the ELM Server

Once you establish a Telnet session in either direction, press ENTER two times. You should receive version information. If you do not receive this message, or if you are unable to connect to the port, check the following:

- On the end that fails, run **netstat -a -p tcp** at a command prompt. This will show all listening ports and connections. You should see the Agent listening on TCP port 1253 and the ELM Server listening on TCP port 1451, or whatever ports you have configured. If you do not see this entry, restart the application on the failed end (either Agent or ELM Server).

- **Does the Agent Status show a registered ELM Server?** From the ELM Server, double-click the Agent and navigate to the Agent Status tab. This will display the Agent's status, which may indicate a problem, such as a failure to execute a monitor item or a failure to communicate with the ELM Server.
- **Is the Agent in cache mode?** If the Agent is unable to transmit data to the ELM Server when it has something to send, the Agent will go into cache mode. Each time the Agent has something new to send (e.g., a new event or alert), it checks to see if it can connect to the ELM Server. If it can, it will dump its cache. The Agent Status tab can display whether or not an Agent is in cache mode.
- **Is the ELM Server running on NT Workstation, Windows 2000 Professional or Windows XP?** These operating systems have a hard-coded limit of 10 inbound TCP/IP connections. Once there are 10 established connections, no new connections will be able to be established until one or more connections is freed up. You can use the **netstat** command to count the number of TCP/IP connections in use. The suggested resolution is to upgrade to a Windows Server family product.

If none of these solutions resolves your issue, please contact TNT Software's [Product Support Group](#) for assistance.

Monitor Items

Creating and Using Monitor Items

Monitor Items are individual items that you want to monitor or collect. For example, to collect performance data from a Windows NT, Windows 2000, Windows XP or Windows 2003 computer, you would use a Performance Collector. To monitor performance and be notified of potential problems, you would use a Performance Alarm.

ELM Performance Manager includes several Monitor Items:

- **Agent Monitor.** This is used to monitor an ELM Service Agent. Agent Monitors perform regular heartbeat checks on Service Agents. If the Server Agent does not respond or is slow in responding, a variety of actions and notification options can be triggered.
- **ELM Server Monitor.** This is used to enable a Service Agent to monitor availability of the ELM Server.
- **Performance Alarm.** Performance Alarms monitor performance objects, counters and instances and can generate a variety of Notification Methods when a counter or instance of a counter is greater than, less than or equal to your specified threshold for your specified duration.
- **Performance Collector.** This Monitor Item is used to collect and store performance data from Windows NT, Windows 2000, Windows XP and Windows 2003. A Performance Collector is a group of performance counters that are collected at the same time. You can use multiple Performance Collectors that contain different groups of counters, or a single Performance Collector that contains all of the counters you want to collect.
- **Process Monitor.** If you need to monitor individual processes, you can do so with a Process Monitor. The Process Monitor is multi-functional; it can let you know when a process has exceeded the threshold of CPU usage you specify, and it can track when processes are instantiated or terminated.
- **WMI Monitor.** If you are using Windows Management Instrumentation--the Microsoft implementation of Web-Based Enterprise Management (WBEM)--you can use WMI Monitors to query a WMI namespace and database. If the results of the query change, a variety of actions and notification options can be executed.

Some Monitor Items also include a checkbox for 'Default.' When checked, this monitor item will automatically be assigned to any new (appropriate) Agents that you create.

Monitor Item Best Practices

Below are some guidelines for using Monitor Items:

- Only Service Agents can execute Monitor Items in real-time. For Remote Agents, we recommend a Scheduled Interval of 10 seconds or greater.
- Disabled Monitor Items do receive some cycles from the ELM Server, so for best performance you should keep the number of disabled Monitor Items to a minimum.
- Assign multiple similar Monitor Items sparingly. If you assign multiple Event Collectors, you may receive unwanted events, or receive the same events multiple times.
- Some Monitor Items include the ability to execute Actions. Leverage this for additional management power!
- When using Remote Agents, the Monitor Items are executed remotely by the ELM Server. You can use the ELM Server's performance object to get metrics on the Monitor Item job queue.

Creating Monitor Items

ELM Server Monitor

An ELM Server Monitor enables **Service Agents** to perform regular heartbeat checks on the ELM Server. If the ELM Server does not respond or is slow in responding, a variety of actions and notification options can be triggered.

You can configure the ELM Server Monitor to restart the ELM Server by putting a check in the **Attempt to restart the ELM Server when the heartbeat check fails** checkbox. When an ELM Server is shutdown gracefully, a flag is written to the Windows registry on the ELM Server computer:

```
HKLM\Software\TNT Software\<ELM Product>\3.1\Settings\NormalShutdown = 0x0000001 (1)
```

A value of 1 indicates a normal shutdown. When the ELM Server service is restarted, this flag (e.g., the NormalShutdown value) is removed from the registry. Before a Service Agent will attempt to restart a stopped ELM Server it will read the registry to see if the flag is present. If the flag exists, the Service Agent will not attempt to restart the ELM Server. If the flag does not exist, the Service Agent will attempt to restart the ELM Server (if configured to do so).

Note

If you want the Service Agent to restart a stopped ELM Server, the Service Agent must run under a user account with administrative rights on the ELM Server (e.g., rights sufficient to enable it to start a service). In addition, because restarting the ELM Server requires the reading of a registry setting on the ELM Server computer, the Service Agent must have remote access to the ELM Server's registry with the appropriate permissions to determine whether or not the NormalShutdown flag is present.

By default, a warning event will be generated if the ELM Server response takes longer than 5 seconds. If the Service Agent and the ELM Server communicate over slow or very busy network links, you should consider increasing this value. To do this, simply change the value in the **Warn if slower than __ seconds** from 5 to the desired amount.

To generate a warning each time the response is slower than the number of seconds specified, check the box that says **Continue to warn after first failure**. If you only want to be notified the first time the ELM Server responds slower than the number of seconds specified, uncheck this box.

How To Create an ELM Server Monitor

An ELM Server Monitor enables **Service Agents** to perform regular heartbeat checks on the ELM Server. Service Agents assigned this Monitor Item will attempt socket connections at the configured intervals. If the socket connection attempt fails, the Service Agent will look for the presence of the NormalShutdown registry flag to determine whether or not to restart the ELM Server.

If the ELM Server does not respond or is slow in responding, a variety of actions and notification options can be triggered.

» To create an ELM Server Monitor

1. Right-click on the **Monitor Items** container in the ELM Console and select **All Tasks | New Monitor Item**. The Create Monitor Wizard will appear. Click **Next** to continue.
2. Select **ELM Server Monitor** from the Monitor Type dropdown and click **Next** to continue.
3. Configure the ELM Server Monitor settings.
 - You can have the Service Agent attempt to restart a stopped ELM Server by checking the **Attempt to restart ELM Server when heartbeat check fails** checkbox.
 - By default, a warning event will be generated if the ELM Server response takes longer than 5 seconds. If the Service Agent and the ELM Server communicate over slow or very busy network links, you should consider increasing this value to 15 or 20 seconds. You may need to experiment with this value to determine the appropriate setting for your environment. To do this, change the value in the **Warn if slower than ___ seconds** from 5 to the desired amount.
 - To generate a warning each time the response is slower than the number of seconds specified, check the box that says **Continue to warn after first failure**. If you only want to be notified the first time the Service Agent responds slower than the number of seconds specified, uncheck this box.
4. Click **Next** to continue. The Monitor Action dialog will appear. When the state, value or condition of a monitored item changes, you can specify what Actions are to be taken. Select the Monitor Action(s) you want to use and click Next to continue.
5. You can test the ELM Server Monitor before using it. To do this, select a Service Agent from the Agent dropdown, select the Action or condition you want to test, and click the **Start Test** button. When testing the ELM Server Monitor, the Service Agent must be running under a user account with administrative rights on the ELM Server. Note that the test does not actually restart the ELM Server service.
6. Click **Next** to continue. The Agents dialog box will appear. Check the checkbox for each Service Agent to which you want to apply the ELM Server Monitor.
7. Click **Next** to continue. The Schedule dialog box will appear.
 - On the Scheduled Interval tab, set the frequency at which you want to execute this ELM Server Monitor.
 - On the Scheduled Hours tab, configure the hours and days you want this ELM Server Monitor active.
8. Give the ELM Server Monitor any desired **Name** and **Description**. Leave the Enabled checkbox checked to activate the ELM Server Monitor immediately. If you want this ELM Server Monitor assigned to all newly created Service Agents, then check the box that says **Make this item a default selection for new items**.
9. Click **Finish** to save the ELM Server Monitor.

Performance Alarms

A Performance Alarm is a condition where a selected performance counter, or instance of a counter, is less than, greater than, or equal to a specific value. Performance Alarms specify what action is to be taken when a performance counter or instance meets the specified criteria.

Performance Alarms are a great way to proactively manage your Windows systems. By configuring Alarms, you'll be able to take action at the first sign of trouble. You can configure Alarms to send email messages and network messages, and even execute commands, batch files and applications.

How To Create a Performance Alarm

Performance Alarms monitor performance objects, counters and instances and can generate a variety of Notification Methods when a counter or instance of a counter is greater than, less than or equal to your specified threshold for your specified duration.

» To create a Performance Alarm:

1. Right-click on the **Monitor Items** container in the ELM Console and select **All Tasks | New Monitor Item**. The Create Monitor Wizard will appear. Click **Next** to continue.
2. Select **Performance Alarm** from the Monitor Type dropdown and click **Next** to continue.
3. Enter a **Name** and **Description** and click **Next** to continue.
4. The Performance Alarm Watch dialog box will appear.
 - a. In the **Object** drop-down, select the **Performance Object** you want to monitor. If the object you want to monitor is not listed, you can add additional objects and counters by clicking the **Add** button and following these **instructions**.
 - b. In the **Counter** drop-down, select the **Performance Counter** you want to monitor.
 - c. To monitor all instances of a particular counter, leave an asterisk in the **Instances** field. To monitor a single instance, or a specific set of instances, click the **Add/Remove** button, enter the instance(s) you want to monitor and click **Close**. Alternatively, you can enter multiple instances directly in the **Instances** field; be sure to separate each instance with a semi-colon.
 - d. In the **Condition** field, enter the condition you want to match (e.g., less than, greater than, equal to, and so forth).
 - e. Enter the value you want to match in the **Value** field.
 - f. In the **Occurs** field, enter the number of consecutive times this condition can be met before triggering notification.
5. Click **Next** to continue. The Monitor Action dialog will appear. When the state, value or condition of a monitored item changes, you can specify what Actions are to be taken. Select the Monitor Action(s) you want to use and click **Next** to continue.
6. The Test Monitor Item dialog box will appear enabling you to test the Performance Alarm before using it. To do this, select an Agent on from the Agent dropdown and click the **Start Test** button.
7. Click **Next** to continue. The Agents dialog box will appear. Check the checkbox for each Service Agent to which you want to apply the Performance Alarm.

8. Click **Next** to continue. The Schedule dialog box will appear.
 - On the Scheduled Interval tab, set the frequency at which you want to execute the Alarm. Leaving the interval at the default of 1 second will enable you to monitor the performance counter or object in real-time.
 - On the Scheduled Hours tab, configure the hours and days you want this monitor active.
9. Click **Finish** to save the Performance Alarm.

Performance Collector

Performance Collectors are sets of one or more performance objects, counters and/or instances that are grouped together for collection and aggregation. ELM Performance Manager and ELM Performance Manager come pre-populated with a variety of Performance Collectors. You can edit any of these or create your own custom Performance Collectors. Each Performance Collector is comprised of three parts: the counters being collected; the frequency of the collection (e.g., every 30 minutes, every hour, etc.); and the days on which collection occurs.

ELM comes pre-populated with a variety of Performance Objects and Counters. If the object, counter or instance you want to collect or monitor is not listed, you can very easily add it from a Windows NT, Windows 2000, Windows XP or Windows 2003 computer that publishes the counter.

How To Use Performance Collectors

Performance Collectors are used to collect and store performance data from Windows NT, Windows 2000, Windows XP and Windows 2003. A Performance Collector is a group of performance counters that are collected at the same time. You can use multiple Performance Collectors that contain different groups of counters, or a single Performance Collector that contains all of the counters you want to collect.

» To use Performance Collector:

1. Right-click on the **Monitor Items** container in the ELM Console and select **All Tasks | New Monitor Item**. The Create Monitor Wizard will appear. Click **Next** to continue.
2. Select **Performance Collector** from the Monitor Type dropdown and click **Next** to continue.
3. Enter a **Name** and **Description** and click **Next** to continue.
4. The Performance Counter dialog box will appear. The initial view of this field will be a list of defined **Performance Object**. If the object you want to monitor is not listed, you can add additional objects and counters by following these **instructions**. Expand each object containing counters you want to monitor and put a check in the box for each **Performance Counter** you want to collect.
5. Click **Next** to continue. The Summary dialog box will appear. Use this dialog box to aggregate (e.g., average) the collected data. Aggregating data is a great way to manage the size of the database used to store the collected performance data. An aggregated database will contain detailed data for the most recent collection period and summary data for historical periods. Data can be aggregated every week, once a month or once a quarter, or you can turn it off completely.
 - a. Use the **On** field to select the day on which aggregation will take place.
 - b. Use the **At** field to specify the time.

Note

You do not need to aggregate your data. This feature is intended as a convenience for those customers who need to minimize the size or growth of their performance data database. Aggregating (summarizing) on a weekly basis, for example, will replace a week's worth of data with an average for that week. If you need to maintain specific counter data for all collection intervals, do not aggregate the data.

6. Click **Next** to continue. The Test Monitor Item dialog box will appear enabling you to test the Performance Collector before using it. To do this, select an Agent on from the Agent dropdown and click the **Start Test** button.
7. Click **Next** to continue. The Agents dialog box will appear. Check the checkbox for each Agent to which you want to apply the Monitor Item.
8. Click **Next** to continue. The Schedule dialog box will appear.
 - On the Scheduled Interval tab, set the frequency at which you want to collect the performance data.
 - On the Scheduled Hours tab, configure the hours and days you want performance data collection active.
9. Click **Finish** to save the Performance Collector.

Process Monitor

As its name implies, the Process Monitor is used to monitor processes on an Agent. The Process Monitor is multi-functional; it can let you know when a process has exceeded the threshold of CPU usage you specify, and it can track when processes are instantiated or terminated. In addition, it can generate a Warning or Error when the number of instances of a particular process exceeds your custom value.

Each Process Monitor item supports multiple matches. Use the **Add** button to add an additional match. Use the **Delete** button to remove a listed match. **Double-click** any listed item to edit it.

You can use the asterisk (*) as a wildcard character, a pipe (|) as an OR operator, the ampersand (&) as an AND operator, and the exclamation point (!) as a NOT operator. For example, to monitor all processes except the *System Idle* process and the *_Total (All)* process, use the following syntax:

!!Idle&!_Total (All)

You can generate a Warning event when CPU utilization by a monitored process meets or exceeds the value specified in the **Warning when % Processor Time is Greater Than** field, and you can generate an Error event when CPU utilization by a monitored process meets or exceeds the value specified in the **Error when % Processor Time is Greater Than** field. By default, a Warning is generated when any process uses more than 50% of the CPU time, and an error is generated when any process uses more than 75% of the CPU time.

Process Monitors can also notify you when a process is instantiated, or when a running process terminates. These settings can be found on the **New Process** and **Process Ended** tabs of the Process Monitor's Monitor Action dialog box.

You can also be alerted when the number of instances of any process exceeds your specified Process Count. Use the **Warning when Process Count is greater than** and **Error when Process Count is greater than** fields to specify Process Count thresholds.

How To Create a Process Monitor

If you need to monitor individual processes, you can do so with a Process Monitor. The Process Monitor is multi-functional; it can let you know when a process has exceeded the threshold of CPU usage you specify, when any process is instantiated or terminated, or when the number of instances of any process exceeds a specified threshold.

» To create a Process Monitor:

1. Right-click on the **Monitor Items** container in the ELM Console and select **All Tasks | New Monitor Item**. The Create Monitor Wizard will appear. Click **Next** to continue.
2. Select **Process Monitor** from the Monitor Type dropdown and click **Next** to continue.
3. Enter a **Name** and **Description** and click **Next** to continue.
4. The Process Monitor Definition dialog box will appear.

- a. Click the **Add** button to add a process to be monitored. The Add Process Name dialog box will appear. Enter the name of the process you want to monitor. You can use the asterisk (*) as a wildcard character, a pipe (|) as an OR operator, the ampersand (&) as an AND operator, and the exclamation point (!) as a NOT operator.

For example, to monitor all processes *except* the *System Idle* process and the *_Total* process, use the following syntax:

!Idle&!_Total

- b. Use the **Delete** button to remove a listed match.
 - c. **Double-click** any listed item to edit it.
 - d. You can execute a Warning action when CPU utilization by a monitored process meets or exceeds the value specified in the **Warning when % Processor Time Greater Than** field.
 - e. You can execute an Error action when the CPU utilization by a monitored process meets or exceeds the value specified in the **Error when % Processor Time Greater Than** field.
 - f. You can execute a Warning action when the number of instances of a given process exceeds your specified Process Count threshold in the **Warning when Process Count is greater than** field.
 - g. You can execute an Error action when the number of instances of a given process exceeds your specified Process Count threshold in the **Error when Process Count is greater than** field.
5. Click **Next** to continue. The Monitor Action dialog will appear. When the state, value or condition of a monitored item changes, you can specify what Actions are to be taken. Select the Monitor Action(s) you want to use and click **Next** to continue.
 6. The Test Monitor Item dialog box will appear enabling you to test the Process Monitor before using it. To do this, select an Agent on from the Agent dropdown and click the **Start Test** button.
 7. Click **Next** to continue. The Agents dialog box will appear. Check the checkbox for each Service Agent to which you want to apply the Process Monitor.
 8. Click **Next** to continue. The Schedule dialog box will appear.

- On the Scheduled Interval tab, set the frequency at which you want to execute this Process Monitor.
- On the Scheduled Hours tab, configure the hours and days you want this Process Monitor active.

9. Click **Finish** to save the Process Monitor.

WMI Monitor

The WMI Monitor periodically queries the Windows Management Instrumentation database, alerting you when the results of the query change. Windows Management Instrumentation (WMI) is Microsoft's implementation of a Web-Based Enterprise Management (WBEM)-compliant model that supports uniform system and applications management.

WMI is based on the Common Information Model adopted by the Distributed Management Task Force. WMI is a key component of Microsoft Windows management services, and an integral part of Windows 2003, Windows 2000, and Windows XP. WMI is also available for Windows NT from [here](#).

Monitoring with a WMI monitor item is accomplished using a query of the WMI namespace (typically **root\cimv2**). This query, which you must manually formulate and enter, can be created using VBScript or JScript.

In the **Namespace** field, enter the name of the WMI namespace that you want to query.

Note

We recommend that you leave this at the default setting. Unless you have manually changed your WMI namespace, the default for Windows systems is root\cimv2.

In the **Query** field, enter the query you wish to execute.

The first time the query is run, the results are logged. If on any subsequent query the results are different, you can trigger one of several Actions: an Alert, a customizable Warning event in the Application log, a customizable network message, or a batch file, executable or script.

How To Create a WMI Monitor

If you are using **Windows Management Instrumentation**--the Microsoft implementation of Web-Based Enterprise Management (WBEM)--you can use WMI Monitors to query a WMI namespace and database. If the results of the query change, a variety of notification options can be executed. WMI monitor items periodically query the Windows Management Instrumentation database and generate alerts when the results of the query change.

» To create a WMI Monitor:

1. Right-click on the **Monitor Items** container in the ELM Console and select **All Tasks | New Monitor Item**. The Create Monitor Wizard will appear. Click **Next** to continue.
2. Select **WMI Monitor** from the Monitor Type dropdown and click **Next** to continue.
3. Enter a **Name** and **Description** and click **Next** to continue.

4. The Windows Management Instrumentation Monitor dialog box will appear.
 - a. In the **Namespace** field, enter the name of the WMI namespace that you want to query. Unless you have manually changed your WMI namespace, the default for Windows systems is root\cimv2.
 - b. In the **Query** field, enter the query you wish to execute. The first time the query is run, the results are logged. If on any subsequent query the results are different, you can trigger one of several notification methods: an Alert, a customizable Warning event in the Application log, a network message or a batch file, executable or script.
5. Click **Next** to continue. The Monitor Action dialog will appear. When the state, value or condition of a monitored item changes, you can specify what Actions are to be taken. Select the Monitor Action(s) you want to use and click **Next** to continue.
6. The Test Monitor Item dialog box will appear enabling you to test the WMI Monitor before using it. To do this, select an Agent on from the Agent dropdown and click the **Start Test** button.
7. Click **Next** to continue. The Agents dialog box will appear. Check the checkbox for each Service Agent to which you want to apply the WMI Monitor.
8. Click **Next** to continue. The Schedule dialog box will appear.
 - On the Scheduled Interval tab, set the frequency at which you want to execute this WMI Monitor.
 - On the Scheduled Hours tab, configure the hours and days you want this WMI Monitor active.
9. Click **Finish** to save the WMI Monitor.

Monitor Item Actions

In ELM Performance Manager, many Monitor Items all include the ability to generate notification and/or execute Actions. There are four 'Actions' that can be executed by a Monitor Item:

- Create a New Alert Entry
- Create an Application Event Log Entry
- Send a Network Message
- Run a command

When the state of a monitor item changes, you can specify what actions are to be taken. These actions - also called Notification Methods - are intended to alert an administrator to the monitor item state change, take corrective action, or both. You have four actions that are available to you:

- **Create New Alert Entry.** Selecting this checkbox to cause an Alert to be generated and posted to the Alerts container within the Console snap-in.
- **Create Application Event Log Entry.** Selecting this enables you to cause a customizable event to be logged to the Application log on the ELM Server.
- **Net Send Message.** Using this option enables you to send a popup message over the network. The target system must have the Messenger Service (Windows NT, Windows 2000, Windows 2003, or Windows XP) or WinPopUp (Win9x/WinMe) running in order to receive the Net Send Message. Use the **Browse** button to browse for a target computer, or manually enter the name of the computer to which you want to send messages in the **Computer Name** field.

Note

The Message field that appears on this dialog applies to the above actions. Use the **Variables** button to specify any additional variables you want the event to include.

- **Run Command.** This option provides a mechanism for executing a batch file, running a command line application or launching a script (CScript or WScript). Use the **Edit** button to create and edit any scripts or command line parameters you want to execute.

Event Filters, Rules and Notification Methods

Using ELM Performance Manager as a Rules-Based Management System

At its core, ELM is a Rules-Based Management System. **Rules** tie together **Event Filters** and **Notification Methods**. Using Event Filters and Rules, you decide which Alerts and conditions trigger notification or corrective action.

Event Filters can be applied to Rules, which associate user-defined Notification Methods with Event Filters. This provides the ability for an administrator to be contacted when important events occur. Using Event Filters, you can define which Alerts are important without having to define each individual Alert. Event Filters can also be created using wildcards and Boolean logic on any information in the Alert.

ELM comes pre-populated with a number of rules that help you manage your environment. These rules enable you to manage your Windows workstations and servers right out-of-the-box, without the need for any add-ons, scripts or other software.

Event Filters

Event Filters are used to isolate one or more specific Alerts. Event Filters provide a mechanism for selecting a subset of all Alerts. Using wild cards and Boolean logic, the filter will identify an event or group of events. Any number of Event Filters can be combined. By using wildcards and Boolean operators, the Administrator does not have to be familiar with every Alert that might be generated.

» To create a new Event Filter:

1. Right-click on the **Event Filters** object in the ELM Console, and select **All Tasks | New Event Filter**. This will launch the **Create New Event Filter Wizard**.
2. In the **Event Filter Criteria** dialog box, enter in the event filter criteria you wish to use. Leading and trailing wildcards (*) and character position wildcards (%) are supported, as are the Boolean operators Or (|), And (&), and Not (!).
 - For example, to filter messages from SQL Server you can specify **SQL*** as the event source. This will filter on any event source that begins with the letters **SQL**. To filter SQL events from servers **A**, **B**, and **C** you would specify **A|B|C** in the computer name field.

- Blank fields are ignored in filter processing. For example, if you leave the **Computer Name** field blank, it will be ignored in the filter process, and the filter will apply to all computers.

Note

Make sure there is no white space adjacent to the operators.

3. Click **Next** to continue. The Compliment Event Filter dialog box will appear. If you want the filter applied when an event does NOT match it, check the **Apply When Event Does NOT Match** checkbox. This option is useful when defining an event filter that includes a large number of events by excluding a small set of events.
4. Click **Next** to continue. The Test Event Filter dialog box will appear. Use this dialog to select an event and test the filter to see if the event passes the filter criteria. You can specify the computer, event log, event source and event ID, and provide a custom insertion string to use in your test. You can view whether or not an event matches the filter criteria by examining the Filter Status field after selecting the event you want to test.
5. Click **Next** to continue. The Rules dialog box will appear. Put a checkmark in the box next to each Rule to which you want this filter applied.
6. Click **Next** to continue. Provide the filter with a meaningful **Name** and an optional **Description**, and click **Finish** to save the new Event Filter.

Notification Methods

Notification Methods are the ways you would want to be notified of Alerts that occur. You can have separate methods for various Alert categories, or separate methods for various application Alerts. For example, you could have one method that describes how to notify a database administrator about important database related Alerts, and another method for notifying a security administrator about important security related Alerts.

Notification Methods pass the full Alert information to the notification engine, which in turn forwards that information depending on the methods selected. If desired, you can customize the information sent via the Notification Method. This is helpful if there are any restrictions on message length, as in the case of a mobile pager. Customizable messages are also a convenient way of making the notification more meaningful.

The following describes each of the available methods of notification:

Notification Method	Description
Alert	Alert items are used to create Alerts. Alerts are displayed in the Alerts container, and are visible from any ELM Console.
Beep	This produces a sound on the ELM Server. The frequency and duration of the beep are customizable allowing you to designate different sounds to different types of events.
Forward Event	This is used to send an event from one ELM Server to another. Transmission of the event data is encrypted for security.
E-Mail	You can choose either Simple Mail Transfer Protocol (SMTP) or Messaging API (MAPI) email notification. You can customize several aspects of the message that is sent, including the From field, the message text (including variables and information from any event), and the size of the message. In addition, you can configure the message with compressed white space, which provides better viewing on cell phones, pagers and other SMTP-capable devices with limited view screens.
Instant Message	ELM can send notifications using the MSN protocol to users signed into the Microsoft .NET Messenger Service.
Marquee Device	ELM can send notifications via a serial connection or over TCP/IP to a support electronic sign. You can customize a variety of options regarding the message that is displayed on the sign, including message color, effects, and how long it remains shown on the marquee.
Network Message	You can send customized messages to any Windows systems on your network. The target system must have the Messenger Service (Windows NT, Windows 2000, Windows XP) or the WinPopUp application (Windows 9x, Windows Me) running in order to receive the Network Message. This message is essentially the same as a NET SEND message in Windows.
Pager	You can send events to numeric, alphanumeric, TAP and SMS pagers using the Pager Notification Method and a modem attached to your ELM Server.
Play Sound File	This method plays the selected sound file on the ELM Server. Any audio format supported by the server on which your Server is running can be played. You can even record a custom sound file and use that in this Notification Method.
Post Web Form	This method is useful, for example, to send pager messages through the pager service's web interface, or for posting information to an internal intranet site or to an Internet Web site.
Command Script	You can run a command, a command line application, a batch file, or a script. In addition, you can pass event information in the form of variables, enabling you to leverage information in the event, such as the computer name or the message details field in any batch files or scripts that get executed. You can use cscript and cmd.exe files, as well as other available script engines (perl, python, etc.).
SNMP Trap	The ELM Server can take any event, alert or alarm and re-package it as an SNMP Trap. The event can then be sent to a customer-owned SNMP Management System.
SNMP OID	The ELM Server can write (put) any readable SNMP Object ID (OID). Simply browse the computer for the available OID values, and then configure the value you want written when this notification method is executed.
Syslog	Prior versions of ELM used a separate utility called SendEvent to send events from an ELM Console to a Syslog server. As was the case with SendEvent, when an event is forwarded to a Syslog server, the Syslog server receives the event as if it were sent from the Agent that generated the event.
Text-to-Speech Message	You can have any event read by an electronic voice on the ELM Server. The speech-to-text engine allows you to hear a synthesized human voice that speaks the message that is passed to it. You can pass the event unmodified, or customize it to suit your needs.

Alerts

Alerts are a convenient way to be notified of a critical problem. The flexibility and ease-of-use of Alerts enables administrators to be notified of potential and real problems as quickly as possible.

Alerts originate from two places; they are either generated as an action from a Monitor Item, or from an Alert Notification Method. When an Alert is generated, it appears in the Alerts container in the ELM Console. Alerts that are generated from a Monitor Item's Action tab are processed using Event Filters, and can therefore trigger Rules and Notification Methods. To avoid looping notification, Alerts that are generated using the Alert Notification Method are not processed using Event Filters, and therefore do not trigger Rules or Notification Methods.

Alerts are stored in a table called TNTAlerts that exists in the database used by the ELM Server. Alerts will remain in the Alerts container (and therefore in the Alerts database) until they are manually deleted from this container.

Alerts have two Status settings: **Open** and **Closed**. You can configure the ELM Console to display Alerts based on its status (**Open**, **Closed**, or **Both**). You can also re-open Alerts that have been closed.

How To Create an Alert

As the name implies, the Alert Item Notification Method is used to create Alerts. Alerts are displayed in the Alerts container, and are visible from any ELM Console.

» To create an Alert:

1. Right-click on the **Notification Methods** container in the ELM Console and select **All Tasks | New Notification Method**. The Create Notification Method Wizard will appear. Click **Next** to continue.
2. Select **Create Alert Entry** from the Notification Method dropdown and click **Next** to continue.
3. Enter a **Name** and **Description** and click **Next** to continue.
4. The Test Monitor Item dialog box will appear enabling you to test the Alert before using it. To do this, click the **Test** button.
5. Click **Next** to continue. The **Threshold** dialog box will appear. You can specify three different threshold settings:
 - a. **Disable this notification when it is triggered**. If the Notification Method is triggered the configured number of times within the specified time period, the notifications will stop. The Notification Method is then re-enabled after the time period specified.
 - b. **Activate this notification method after it is triggered**. When this threshold is selected, the notifications will not be processed unless the rule is triggered the specified number of times within the time period selected.
 - c. **Consolidate notifications by waiting until either**. You can configure the Notification Method to wait until being executed until either a specific number of similar events has occurred, or until a specific amount of time has elapsed.
6. If you don't want to be notified for cached data, check the box that says **Disable this notification method for all Cached (old) data**.
7. Click **Next** to continue. The Schedule dialog box will appear. Use your mouse to configure the hours and days you want this Notification Method active.
8. Click **Finish** to save this Notification Method.

Beeps

A Beep Notification Method is used to play a beep sound on the ELM Server computer. You can configure several aspects of the beep sound, enabling you to use different sounding beeps for different events/alerts. The following attributes of a Beep notification can be configured:

- **Repeat Count.** This slider controls how many times the beep sound is repeated.
- **Duration.** Use this slider to specify the duration for each beep sound.
- **Delay.** This is the amount of time in between repeated beeps.
- **Frequency.** This slider controls the frequency of the beep.

How To Create a Beep Notification Method

Beep Notification Methods are used to produce a sound on the ELM Server when an event occurs. The frequency and duration of the beep are customizable allowing you to designate different sounds to different types of events.

» To create a Beep Notification Method:

1. Right-click on the **Notification Methods** container in the ELM Console and select **All Tasks | New Notification Method**. The Create Notification Method Wizard will appear. Click **Next** to continue.
2. Select **Beep** from the Notification Method dropdown and click **Next** to continue.
3. The Beep Settings dialog box will appear enabling you to configure the Beep options. Use the **Test** button to hear how the beep sounds after adjusting one or more of these sliders.
 - **Repeat Count.** This slider controls how many times the beep sound is repeated.
 - **Duration.** Use this slider to specify the duration for each beep sound.
 - **Delay.** This is the amount of time in between repeated beeps.
 - **Frequency.** This slider controls the frequency of the beep.
4. Click **Next** to continue. The **Rules** dialog box will appear. Put a checkmark next to each Rule you want to trigger this Notification Method.
5. Click **Next** to continue. The **Threshold** dialog box will appear. You can specify three different threshold settings:
 - a. **Disable this notification when it is triggered.** If the Notification Method is triggered the configured number of times within the specified time period, the notifications will stop. The Notification Method is then re-enabled after the time period specified.
 - b. **Activate this notification method after it is triggered.** When this threshold is selected, the notifications will not be processed unless the rule is triggered the specified number of times within the time period selected.
 - c. **Consolidate notifications by waiting until either.** You can configure the Notification Method to wait until being executed until either a specific number of similar events has occurred, or until a specific amount of time has elapsed.
6. If you don't want to be notified for cached data, check the box that says **Disable this notification method for all Cached (old) data**.

7. Click **Next** to continue. The Schedule dialog box will appear. Use your mouse to configure the hours and days you want this Notification Method active.
8. Enter a **Name** and **Description** and click **Next** to continue.
9. Click **Finish** to save this Notification Method.

Command Script

The Command Script Notification Method can execute a command, a command line application, a batch file, or a script. In addition, you can pass event information in the form of variables, enabling you to leverage information in the event, such as the computer name or the message details field in any batch files or scripts that get executed. The variables you can use are:

- %Category%
- %Computer%
- %Date%
- %Event%
- %Logname%
- %Message%
- %Source%
- %Time%
- %Type%
- %User%

ELM supports the Windows Script Host and command line (cmd.exe) files. If you want to use execute a different type of script (e.g., a Perl script), enter the name of the script engine in the Type dropdown (e.g., perl.exe).

Command Scripts do not use external batch or script files. The script exists within the Command Script Notification Method, which is stored in the ELM Server's configuration data. When executing a Command Script Notification Method, the ELM Server will create a temporary file in the user TEMP folder within the path of the ELM Server service account's profile. Once the Command Script has been executed, the temporary file will be automatically deleted. In addition, you can launch any valid executable (.exe) file, as well as any file whose extension has an associated program that launches when the file is executed.

How To Create a Command Script Notification Method

The Command Script Notification Method is used to execute a script, batch file, or command line application when triggered. This notification method enables you to trigger action (e.g., take corrective action) when an event, condition or alert occurs. For example, if a critical service stops or terminates unexpectedly, you can use this notification method to restart it. Any action that can be scripted and executed under the ELM Server service account's security context can be used as a Command Script notification method. ELM supports the Windows Script Host (cscript), as well as command line (cmd.exe). If you want to use execute a different type of script (e.g., a Perl script), enter the name of the script engine in the Type dropdown (e.g., perl.exe).

» To create a Command Script Notification Method:

1. Right-click on the **Notification Methods** container in the ELM Console and select **All Tasks | New Notification Methods**. The **Create Notification Method Wizard** will appear. Click **Next** to continue.
2. Select **Command Script** from the **Notification Method** dropdown and click **Next** to continue.
3. The Script Settings dialog box will appear.
 - In the **Script Name** field, give the Script a name. When using scripts, the Type must be a valid script engine for the type of script you want to run. For example, if you are

executing a VB Script called reboot, the script type you would use is cscript.exe. If you are executing a Perl script called Shutdown, the script type you would manually enter is Perl.exe. The script will be copied to a temporary file in the file system and then executed using the script engine specified in the Script Type.

- Using the **Type** dropdown, select the type of script you want to use. You can choose from **cscript.exe** and **cmd.exe**. If you want to use execute a different type of script (e.g., a Perl script), enter the name of the script engine in the Type dropdown (e.g., perl.exe).
- Enter a **Timeout** value for the script. If the script does not complete within the timeout period, it will be considered a failed notification.
- Enter the **Script** you want executed in the field that contains the sample script. You can also modify the sample script, as well. The contents of the script will be written to a file in the file system which will then be executed using the appropriate script engine.

Note

The sample script is a cscript.exe script that demonstrates how to programmatically enable or disable an Agent. For more information on using these types of scripts, see How to Programmatically Enable or Disable Items.

- Click the **Test** button to test the script. Click **Next** to save the script settings.
4. Click **Next** to continue. The **Rules** dialog box will appear. Put a checkmark next to each Rule you want to trigger this Notification Method. Click **Next** to continue.
 5. The **Threshold** dialog box will appear. You can specify three different threshold settings:
 - a. **Disable this notification when it is triggered.** If the Notification Method is triggered the configured number of times within the specified time period, the notifications will stop. The Notification Method is then re-enabled after the time period specified.
 - b. **Activate this notification method after it is triggered.** When this threshold is selected, the notifications will not be processed unless the rule is triggered the specified number of times within the time period selected.
 - c. **Consolidate notifications by waiting until either.** You can configure the Notification Method to wait until being executed until either a specific number of similar events has occurred, or until a specific amount of time has elapsed.
 6. If you don't want to be notified for cached data, check the box that says **Disable this notification method for all Cached (old) data**.
 7. Click **Next** to continue. The **Schedule** dialog box will appear. Use your mouse to configure the hours and days you want this Notification Method active.
 8. Click **Next** to continue. Enter a Name and Description and if desired, check the **Make this a default selection for new items** checkbox.
 9. Click **Finish** to save the item, and click **OK** to acknowledge the item creation.

How To Programmatically Enable or Disable Items

When monitoring Agents, you may find it useful to automatically enable or disable an item when a dependency item fails. For example, say you were monitoring a server on the other side of a router, and the router itself. If the router goes down, it will appear to the ELM Server as if the monitored systems on

the other side of that router are also down. In this case, you can cause the router down events/alerts to trigger the programmatic disabling of items whose monitoring depends on the router being up.

The programmatic enabling and disabling of items is accomplished by using a Command Script Notification Method that executes a VBScript.

» To Programmatically Enable or Disable an Agent from a Command Script Notification Method:

1. Look at the Properties of the Agent you want to enable/disable and copy the item's Index No. (GUID) to the Windows clipboard.
2. Create a new Command Script Notification Method which will be used to enable or disable the item. Give it a name of **Enable OBJECT** or **Disable OBJECT** where **OBJECT** is the name of the object you want to enable/disable. In the **Script Name** field, name the script **Enable.vbs**. Be sure to set the type to **cscript**. Copy and paste the following into the **Script** field:

```
Call Enable_Agent_Object("", "<Item>", True)
Sub Enable_Agent_Object(ByRef SessionPasswordString, _
ByRef ObjectIndexString, ByVal bEnableObject)

On Error Resume Next ' Defer error trapping.

Dim SessionObject
Set SessionObject = CreateObject("EEMSVR.TNTEnterpriseSession")

Call SessionObject.Connect(SessionPasswordString)

Dim ItemObject
Set ItemObject = SessionObject.AgentCollection.Find(ObjectIndexString)

Dim LockItemObject
Set LockItemObject = CreateObject("TNTWZ.TNTItemWriteLockHelper")

Dim ItemCopyObject
Set ItemCopyObject = LockItemObject.LockedItemCopy(ItemObject)

ItemCopyObject.Enabled = bEnableObject
Call LockItemObject.UpdateOriginalItem
End Sub
```

3. In the above script, change **<Item>** to the Index No. for the Agent. This number is a long GUID surrounded by {}. You can get the Index No. for the Agent by examining the Properties tab on the Agent Properties dialog. Do not include the brackets <> used above, but do include the {} brackets that surround the Agent's Index No. **The above script is used to enable items. To disable items, change the word True to False.** Click **OK** to save the Notification Method.
4. Next, create a new Rule that will be used to execute this Notification Method when an event or Alert indicating the router is down is received by the ELM Server. Note that you may need to create an Event Filter to isolate the specific router down event.
5. On the **Notification Methods** tab, put a check in the checkbox next to the Notification Method you created above.
6. On the **Event Filters** tab, put a check in the checkbox next to the Event Filter you created.
7. Click **OK** to save the Rule.

You can programmatically enable and disable other items, as well. Below are scripts that can be used to enable/disable Monitor Items, Rules and Notification Methods:

Monitor Items:

```

Call Enable_Monitor_Object("", "<Item>", True)
Sub Enable_Monitor_Object(ByRef SessionPasswordString, _
ByRef ObjectIndexString, ByVal bEnableObject)

On Error Resume Next ' Defer error trapping.

Dim SessionObject
Set SessionObject = CreateObject("EEMSVR.TNTEnterpriseSession")

Call SessionObject.Connect(SessionPasswordString)

Dim ItemObject
Set ItemObject = SessionObject.MonitorCollection.Find(ObjectIndexString)

Dim LockItemObject
Set LockItemObject = CreateObject("TNTWZ.TNTItemWriteLockHelper")

Dim ItemCopyObject
Set ItemCopyObject = LockItemObject.LockedItemCopy(ItemObject)

ItemCopyObject.Enabled = bEnableObject
Call LockItemObject.UpdateOriginalItem
End Sub

```

The above script is used to enable items. To disable items, change the word True to False.

Rules :

```

Call Enable_Notification_Rule_Object("", "<Item>", True)
Sub Enable_Notification_Rule_Object(ByRef SessionPasswordString, _
ByRef ObjectIndexString, ByVal bEnableObject)

On Error Resume Next ' Defer error trapping.

Dim SessionObject
Set SessionObject = CreateObject("EEMSVR.TNTEnterpriseSession")

Call SessionObject.Connect(SessionPasswordString)

Dim ItemObject
Set ItemObject = SessionObject.NotificationRuleCollection.Find(ObjectIndexString)

Dim LockItemObject
Set LockItemObject = CreateObject("TNTWZ.TNTItemWriteLockHelper")

Dim ItemCopyObject
Set ItemCopyObject = LockItemObject.LockedItemCopy(ItemObject)

ItemCopyObject.Enabled = bEnableObject
Call LockItemObject.UpdateOriginalItem
End Sub

```

The above script is used to enable items. To disable items, change the word True to False.

Notification Methods :

```

Call Enable_Notification_Object("", "<Item>", True)
Sub Enable_Notification_Object(ByRef SessionPasswordString, _
ByRef ObjectIndexString, ByVal bEnableObject)

On Error Resume Next ' Defer error trapping.

```

```

Dim SessionObject
Set SessionObject = CreateObject("EEMSVR.TNTEnterpriseSession")

Call SessionObject.Connect(SessionPasswordString)

Dim ItemObject
Set ItemObject = SessionObject.NotificationCollection.Find(ObjectIndexString)

Dim LockItemObject
Set LockItemObject = CreateObject("TNTWZ.TNTItemWriteLockHelper")

Dim ItemCopyObject
Set ItemCopyObject = LockItemObject.LockedItemCopy(ItemObject)

ItemCopyObject.Enabled = bEnableObject
Call LockItemObject.UpdateOriginalItem
End Sub

```

The above script is used to enable items. To disable items, change the word **True** to **False**.

Forward Event

An ELM Server can forward any event, Syslog message or SNMP trap to another ELM Server by using the Forward Event Notification Method. Forwarding events from one ELM Server to another enables you to architect and deploy ELM in a tiered manner, or when you are monitoring multiple locations. Use this dialog to configure the event forwarding settings. All communication between the upstream and the downstream ELM Servers is encrypted.

How To Forward an Event

The Forward Event Notification Method is used to forward an event from one ELM Server to another.

» To Forward an Event to an ELM Server:

1. Right-click on the **Notification Methods** container in the ELM Console and select **All Tasks | New Notification Method**. The Create Notification Method Wizard will appear. Click **Next** to continue.
2. Select **Forward Event** from the Notification Method dropdown and click **Next** to continue.
3. The ELM Server Computer Name dialog box will appear.
 - In the **TCP Port** field, enter the port on which the upstream server is listening. By default, ELM Servers listen on the following TCP ports:
 - ☐ ELM Performance Manager - TCP Port 1251
 - ☐ ELM Log Manager - TCP Port 1351
 - ☐ ELM Performance Manager - TCP Port 1451
 - Click the **Add** button to add an upstream server. The **Select Computer** dialog box will appear. You can manually enter the server name in the **Computer Name** field or browse the network and select the server. Click **OK** to add the server. Repeat this step for each upstream server you want to add.
 - Click the **Test** button to verify connectivity. An informational success message will appear, indicating that the message was sent and received successfully.
4. Click **Next** to continue. The **Rules** dialog box will appear. Put a checkmark next to each Rule you want to trigger this Notification Method. Click **Next** to continue.

5. Click **Next** to continue. The **Threshold** dialog box will appear. You can specify three different threshold settings:
 - a. **Disable this notification when it is triggered.** If the Notification Method is triggered the configured number of times within the specified time period, the notifications will stop. The Notification Method is then re-enabled after the time period specified.
 - b. **Activate this notification method after it is triggered.** When this threshold is selected, the notifications will not be processed unless the rule is triggered the specified number of times within the time period selected.
 - c. **Consolidate notifications by waiting until either.** You can configure the Notification Method to wait until being executed until either a specific number of similar events has occurred, or until a specific amount of time has elapsed.
6. If you don't want to be notified for cached data, check the box that says **Disable this notification method for all Cached (old) data**.
7. Click **Next** to continue. The Schedule dialog box will appear. Use your mouse to configure the hours and days you want this Notification Method active.
8. Click **Finish** to save this Notification Method.

You can use the **Remove All** button to remove all of the entries, or select an individual entry and click **Remove** to remove a single entry.

Note

You cannot edit an entry after it is listed in this list. If you make a mistake you need to first remove the entry (using the Remove button) and then re-add the correct entry.

Instant Message

ELM includes support for Microsoft's .NET Messenger Service as a Notification Method.

In order to use an Instant Message Notification Method, you must have the following:

1. A .NET Messenger Service Sign-In Account and Password for the ELM Server service.
2. A .NET Messenger Service Address for each Instant Message Recipient.
3. The ELM Server and the ELM Server service account must have access to the Internet.

For sending instant messages, ELM does not require the installation or use of a .NET Messenger Service client (e.g., Windows Messenger or MSN Messenger) on the ELM Server. However, in order for the recipient to receive the Instant Message from the ELM Server, they must be running one of these clients and signed into the .NET Messenger Service. In addition, they must allow the ELM Server's .NET Messenger Service sign-in account to send them Instant Messages (e.g., either by adding the account to their contact list, or by allowing those who are not on their contact list to send them instant messages).

How To Use an Instant Message Notification Method

ELM uses the MSN Protocol over the [.NET Messenger Service](#) for sending instant messages as a Notification Method. In order to use an Instant Message Notification Method, you must have the following:

1. A .NET Messenger Service Sign-In Account and Password for the ELM Server service.
2. A .NET Messenger Service Sign-In Account and Password for each Instant Message Recipient.
3. The ELM Server and the ELM Server service account must have access to the Internet.

Note

You do not need to install the Windows Messenger or MSN Messenger client on your ELM Server in order to use this notification method. ELM programmatically communicates with the .NET Messenger Service using its native protocol, and therefore does not need the client components.

» To create an Instant Message Notification Method:

1. Right-click on the **Notification Methods** container in the ELM Console and select **All Tasks | New Notification Method**. The Create Notification Method Wizard will appear. Click **Next** to continue.
2. Select **Instant Message** from the Notification Method dropdown and click **Next** to continue.
3. The .NET Messenger Service Sign-In dialog box will appear. Enter the .NET Messenger Service **Sign-In Name** and **Password**. When sending instant messages, the ELM Server will log on to the .NET Messenger Service using this account. The account information is stored in the Windows registry, with the password encrypted for security.
4. Click **Next** to continue. The .NET Messenger Service Recipients dialog box will appear. Enter the address(es) for the .NET Messenger Service recipient(s) and click the **Add** button to add it to the **Recipient List**. Repeat this process for each recipient. To remove an entry from the Recipient List, select the entry and click the **Remove** button.
5. Click **Next** to continue. The .NET Messenger Service Instant Message dialog box will appear. In the **Instant Message** field, Enter the instant message (up to 1,200 characters) that you want to send. Use the **Insert Variable** button to add environmental variables to the message. Use **Ctrl-Enter** to insert a blank line.
6. Click **Next** to continue. The Rule dialog box will appear. Select the Rule(s) you want to use this Notification Method. Click **Next** to continue.
7. The **Threshold** dialog box will appear. You can specify three different threshold settings:
 - a. **Disable this notification when it is triggered**. If the Notification Method is triggered the configured number of times within the specified time period, the notifications will stop. The Notification Method is then re-enabled after the time period specified.
 - b. **Activate this notification method after it is triggered**. When this threshold is selected, the notifications will not be processed unless the rule is triggered the specified number of times within the time period selected.
 - c. **Consolidate notifications by waiting until either**. You can configure the Notification Method to wait until being executed until either a specific number of similar events has occurred, or until a specific amount of time has elapsed.
8. If you don't want to be notified for cached data, check the box that says **Disable this notification method for all Cached (old) data**.
9. Click **Next** to continue. The Schedule dialog box will appear. Use your mouse to configure the hours and days you want this Notification Method active.
10. The Name dialog box will appear. Enter a meaningful name for the Notification Method, and an optional description. If you want this Notification Method to be automatically

applied to all newly created Rules, check the box that says **Make this item a default selection for new items**.

11. Click **Finish** to save this Notification Method.

Mail Notification

ELM supports both **Simple Mail Transfer Protocol (SMTP)** and **Messaging API (MAPI)** email notification. Both Notification Methods enable you to specify the message that gets emailed. In addition, they both allow for configuration of the following message properties:

- **Max Message.** Use this field to specify a maximum message size. By default, the message size is limited to 1,024 characters. Setting a lower value is useful for those email clients/devices (e.g., cell phone, etc.) that have limited viewing size.
- **Compress White Space.** When this box is checked, all white space (CR/LF) will be removed from the message prior to its transmission. This removes line breaks in the message and also helps to reduce message size.

How To Use MAPI Notification

ELM supports the Messaging API (MAPI) for sending MAPI email messages as a Notification Method. In order to use MAPI email, you must have a MAPI-compliant mail client installed on your ELM Server and you must use a MAPI-compliant mail server, such as Microsoft Exchange. Additionally, you must configure the ELM Server service to logon using an account that has access to the mailbox you intend to use, and you must specify the Exchange client as the Default E-Mail client in **Control Panel | Internet Options | Programs | E-mail**.

There are several steps to configuring MAPI email notification.

» To use MAPI email as a Notification Method:

1. Create a **user account** in your NT domain or Active Directory.
2. Create a **mailbox** for this account.
3. Install a MAPI email client on the ELM Server. We recommend using the Microsoft Exchange 5.0 client, however, any version of Outlook will do.
4. Once the email client has been installed, a **MAPI profile** needs to be configured. To do this:
 - Go into **Control Panel | Mail**. The Mail dialog box will be displayed.
 - Click the **Add...** button to create a new profile. Follow the instructions detailed in the Mail Setup Wizard. Note: You must add the Exchange Server service to this profile.
 - Once the profile has been created, make a note of its name. Note: If you do not like the name it assigns, you can quickly rename the profile by copying the newly created profile and giving it a desired name. You should then delete the original profile.
 - Click the **Close** button to exit the Mail dialog box.
5. Next open the **Internet Options** in **Control Panel**. Navigate to the **Programs** tab. In the E-mail field, set the Exchange client (e.g., Microsoft Outlook) as the default e-mail client. Click **OK** to save your changes and close Internet Options.

6. Next, the ELM Server needs to be configured to run using the security context of the account you created in Step 1 above. To do this:
 - a. **Stop** the ELM Server service.
 - b. Using the Windows 2000 Services snap-in, configure the ELM Server to run under the account you created in Step 1.
 - c. **Restart** the ELM Server service.
6. Next, configure the MAPI Notification Method. To do this:
 - a. Log on using the account you created in Step 1.
 - b. Right-click on the Notification Methods container and select **All Tasks | New Notification Method**. The Create Notification Method Wizard will appear. Click **Next** to continue.
 - c. Select **Mail** from the Notification Method dropdown and click **Next** to continue.
 - d. Select **MAPI Email** and click **Next** to continue.
 - e. The MAPI Email Mail Profile dialog box will appear. Select the Logon profile you created in Step 4.
 - f. The Mail Message Settings dialog box will appear.
7. Click **Next** to continue. The **Rules** dialog box will appear. Put a checkmark next to each Rule you want to trigger this Notification Method. Click **Next** to continue.
8. Click **Next** to continue. The **Threshold** dialog box will appear. You can specify three different threshold settings:
 - a. **Disable this notification when it is triggered**. If the Notification Method is triggered the configured number of times within the specified time period, the notifications will stop. The Notification Method is then re-enabled after the time period specified.
 - b. **Activate this notification method after it is triggered**. When this threshold is selected, the notifications will not be processed unless the rule is triggered the specified number of times within the time period selected.
 - c. **Consolidate notifications by waiting until either**. You can configure the Notification Method to wait until being executed until either a specific number of similar events has occurred, or until a specific amount of time has elapsed.
9. If you don't want to be notified for cached data, check the box that says **Disable this notification method for all Cached (old) data**.
10. Click **Next** to continue. The Schedule dialog box will appear. Use your mouse to configure the hours and days you want this Notification Method active.
11. Click **Finish** to save this Notification Method.

How To Create an SMTP Notification Method

You can be notified of any or all events using Simple Mail Transfer Protocol (SMTP)-based email.

» To create an SMTP Notification Method:

1. Right-click on the **Notification Methods** container in the ELM Console and select **All Tasks | New Notification Method**. The Create Notification Method Wizard will

appear. Click **Next** to continue.

2. Select **Mail Notification** from the Notification Method dropdown and click **Next** to continue.
3. The Select Mail Type dialog box will appear. Select **SMTP Mail** from the dropdown. Click **Next** to continue.
4. The SMTP Host dialog box will appear. Enter the IP address, host name, or fully qualified domain name for the SMTP server you want to use in the **SMTP Host** field. If desired, or if required by SMTP server configuration, enter an optional SMTP address in the **From** field.

Note

When using SMTP servers that have been configured to disallow relaying, you will need to use the FROM field. For more servers, using **ELM@yourdomain.com**, where yourdomain.com is a domain that is served by the SMTP server.

5. Click **Next** to continue. The Mail Message dialog box will appear. Enter the address, subject and message details for the email:
 - **To.** Enter the SMTP address(es) for the email recipients. When using multiple recipients, separate entries with a semi-colon (;).
 - **Subject.** Enter the subject you want to use for the email message. You can use the **Insert Variable** button to insert one or more event parameters (e.g., computer name, event ID, event type, etc.) into the Subject line.
 - **Message.** Enter the message you want for the email message. Like the Subject field, you can use the **Insert Variable** button to insert one or more event parameters.
6. Click the **Test** button to test the SMTP Email Notification Method. Once the test has completed successfully, click **Next** to continue.
7. The Mail Message Options dialog box will appear. You can configure two options for email notification methods:
 - **Max Message.** Use this field to specify a maximum message size. By default, the message size is limited to 1,024 characters. Setting a lower value is useful for those email clients/devices (e.g., cell phone, etc.) that have limited viewing size.
 - **Compress White Space.** When this box is checked, all white space (CR/LF) will be removed from the message prior to its transmission. This removes line breaks in the message and also helps to reduce message size.
8. Click **Next** to continue. The Rule dialog box will appear. Select the Rule(s) you want to use this Notification Method. Click **Next** to continue.
9. The **Threshold** dialog box will appear. You can specify three different threshold settings:
 - a. **Disable this notification when it is triggered.** If the Notification Method is triggered the configured number of times within the specified time period, the notifications will stop. The Notification Method is then re-enabled after the time period specified.
 - b. **Activate this notification method after it is triggered.** When this threshold is selected, the notifications will not be processed unless the rule is triggered

the specified number of times within the time period selected.

- c. **Consolidate notifications by waiting until either.** You can configure the Notification Method to wait until being executed until either a specific number of similar events has occurred, or until a specific amount of time has elapsed.
10. If you don't want to be notified for cached data, check the box that says **Disable this notification method for all Cached (old) data**.
11. Click **Next** to continue. The Schedule dialog box will appear. Use your mouse to configure the hours and days you want this Notification Method active.
12. The Name dialog box will appear. Enter a meaningful name for the Notification Method, and an optional description. If you want this Notification Method to be automatically applied to all newly created Rules, check the box that says **Make this item a default selection for new items**.
13. Click **Finish** to save this Notification Method. You will be prompted to create another Notification Method. Select **Yes** or **No** at your discretion.

Marquee Device

ELM includes support for electronic signs (marquees) as a notification method. You can send event and alert information to a supported electronic marquee via TCP/IP or via a serial connection. For a list of supported electronic marquees, please contact TNT Software's [Sales](#) department.

There are five tabs that you can configure, corresponding to the five event types (Error, Warning, Information, Audit Success and Audit Failures). Each tab has the following items that can be configured:

- **Enable.** When this box is checked, the Monitor Item is enabled and will execute as configured. Uncheck this box to disable the Monitor Item.
- **Font.** This is the type of font used in the display. Consult your Marquee's user manual for details on how the fonts look and which fonts are supported.
- **Color.** This is the color of font used in the display. Consult your Marquee's user manual for details on how the fonts look and which fonts are supported.
- **Enable double-height characters.** When this checkbox is checked, the height of the characters is doubled. Consult your Marquee's user guide to see if this is supported.
- **Enable character flash.** When this checkbox is checked, the characters will support flashing (blinking). Consult your Marquee's user guide to see if this is supported.
- **Enable Wide Characters.** When this checkbox is checked, the width of the characters will be widened. Consult your Marquee's user guide to see if this is supported.
- **Message Format.** Use this field to specify and/or customize the message that will be displayed on the Marquee. Use the Insert Variable button to insert one or more event variables.
- **Min Duration.** This is the minimum amount of time the message will be displayed. The message will be visible on the Marquee until the Max Duration value has expired, or until a new message is sent to the Marquee.
- **Max Duration.** This is the maximum amount of time the message will be displayed.

How To Create a Marquee Notification Method

» To create a **TCP / IP** Marquee Notification Method:

1. Right-click on the Notification Methods container in the ELM Console and select **All Tasks | New Notification Methods**. The **Create Notification Method Wizard** will appear. Click **Next** to continue.
2. Select **Marquee Display** from the Notification Method dropdown and click **Next** to continue.
3. The **Marquee Connection Settings** dialog will appear. Select **TCP / IP Connection** and click **Next** to continue.
4. Enter the **Name** or **IP Address** of your Marquee Device and the **TCP Port** it is listening on. Click **Next** to continue.
5. The **Marquee Display Properties** dialog box will appear. Enter the **Display ID**, and configure the Marquee scroll and display settings as desired. Click **Next** to continue.
6. The **Marquee Message Display Settings** dialog box will appear. There are five tabs that you can configure, corresponding to the five event types (Error, Warning, Information, Audit Success and Audit Failures). Each tab has the following items that can be configured:
 - a. **Enable**. When this box is checked, the Monitor Item is enabled and will execute as configured. Uncheck this box to disable the Monitor Item.
 - b. **Font**. This is the type of font used in the display. Consult your Marquee's user manual for details on how the fonts look and which fonts are supported.
 - c. **Color**. This is the color of font used in the display. Consult your Marquee's user manual for details on how the fonts look and which fonts are supported.
 - d. **Enable double-height characters**. When this checkbox is checked, the height of the characters is doubled. Consult your Marquee's user guide to see if this is supported.
 - e. **Enable character flash**. When this checkbox is checked, the characters will support flashing (blinking). Consult your Marquee's user guide to see if this is supported.
 - f. **Enable Wide Characters**. When this checkbox is checked, the width of the characters will be widened. Consult your Marquee's user guide to see if this is supported.
 - g. **Message Format**. Use this field to specify and/or customize the message that will be displayed on the Marquee. Use the Insert Variable button to insert one or more event variables.
 - h. **Min Duration**. This is the minimum amount of time the message will be displayed. The message will be visible on the Marquee until the Max Duration value has expired, or until a new message is sent to the Marquee.
 - i. **Max Duration**. This is the maximum amount of time the message will be displayed.
7. Click the **Test** button to test the notification method.
8. The **Threshold** dialog box will appear. You can specify three different threshold settings:
 - a. **Disable this notification when it is triggered**. If the Notification Method is triggered the configured number of times within the specified time period, the notifications will stop. The Notification Method is then re-enabled after the time period specified.
 - b. **Activate this notification method after it is triggered**. When this threshold is selected, the notifications will not be processed unless the rule is triggered the specified number of times within the time period selected.

- c. **Consolidate notifications by waiting until either.** You can configure the Notification Method to wait until being executed until either a specific number of similar events has occurred, or until a specific amount of time has elapsed.
9. If you don't want to be notified for cached data, check the box that says **Disable this notification method for all Cached (old) data**.
10. Click **Next** to continue. The **Schedule** dialog box will appear. Use your mouse to configure the hours and days you want this Notification Method active.
11. Click **Next** to continue. Enter a **Name** and **Description** and if desired, check the box that says **Make this a default selection for new items**.
12. Click **Finish** to save the Notification Method.

» To create a **Serial Port** Marquee Notification Method:

1. Right-click on the Notification Methods container in the ELM Console and select **All Tasks | New Notification Methods**. The **Create Notification Method Wizard** will appear. Click **Next** to continue.
2. Select **Marquee Display** from the Notification Method dropdown and click **Next** to continue.
3. The **Marquee Connection Settings** dialog will appear. Select **Serial Port Connection** and click **Next** to continue.
4. Select the **COM Port**, **Baud Rate**, **Parity**, **Data Bits** and **Stop Bits** for your Marquee Device. Click **Next** to continue.
5. The **Marquee Display Properties** dialog box will appear. Enter the **Display ID**, and configure the Marquee scroll and display settings as desired. Click **Next** to continue.
6. The **Marquee Message Display Settings** dialog box will appear. There are five tabs that you can configure, corresponding to the five event types (Error, Warning, Information, Audit Success and Audit Failures). Each tab has the following items that can be configured:
 - a. **Enable.** When this box is checked, the Monitor Item is enabled and will execute as configured. Uncheck this box to disable the Monitor Item.
 - b. **Font.** This is the type of font used in the display. Consult your Marquee's user manual for details on how the fonts look and which fonts are supported.
 - c. **Color.** This is the color of font used in the display. Consult your Marquee's user manual for details on how the fonts look and which fonts are supported.
 - d. **Enable double-height characters.** When this checkbox is checked, the height of the characters is doubled. Consult your Marquee's user guide to see if this is supported.
 - e. **Enable character flash.** When this checkbox is checked, the characters will support flashing (blinking). Consult your Marquee's user guide to see if this is supported.
 - f. **Enable Wide Characters.** When this checkbox is checked, the width of the characters will be widened. Consult your Marquee's user guide to see if this is supported.
 - g. **Message Format.** Use this field to specify and/or customize the message that will be displayed on the Marquee. Use the Insert Variable button to insert one or more event variables.
 - h. **Min Duration.** This is the minimum amount of time the message will be displayed. The message will be visible on the Marquee until the Max Duration value has expired, or until a new message is sent to the Marquee.
 - i. **Max Duration.** This is the maximum amount of time the message will be displayed.

7. Click the **Test** button to test the notification method.
8. Click **Next** to continue. The **Rules** dialog box will appear. Put a checkmark next to each Rule you want to trigger this Notification Method. Click **Next** to continue.
9. The **Threshold** dialog box will appear. You can specify three different threshold settings:
 - a. **Disable this notification when it is triggered.** If the Notification Method is triggered the configured number of times within the specified time period, the notifications will stop. The Notification Method is then re-enabled after the time period specified.
 - b. **Activate this notification method after it is triggered.** When this threshold is selected, the notifications will not be processed unless the rule is triggered the specified number of times within the time period selected.
 - c. **Consolidate notifications by waiting until either.** You can configure the Notification Method to wait until being executed until either a specific number of similar events has occurred, or until a specific amount of time has elapsed.
10. If you don't want to be notified for cached data, check the box that says **Disable this notification method for all Cached (old) data**.
11. Click **Next** to continue. The **Schedule** dialog box will appear. Use your mouse to configure the hours and days you want this Notification Method active.
12. Click **Next** to continue. Enter a **Name** and **Description** and if desired, check the box that says **Make this a default selection for new items**.
13. Click **Finish** to save the Notification Method.

Network Message Settings

You can send customized messages to any Windows systems on your network. The target system must have the Messenger Service (Windows NT, Windows 2000, Windows XP and Windows 2003) or the WinPopUp application (Windows 9x, Windows Me) running in order to receive the Network Message. This message is essentially the same as a NET SEND message in Windows.

In the **Computer Name** field, enter the NetBIOS name of the computer to which you want the message sent. You can use the **Browse** button to browse your network for a computer. If you want to send the Network Message to the computer that generated the Event/Alert, you can use **%computer%** in the Computer name field.

In the **Message** field, enter the message you want transmitted. You can completely customize the message. Use the **Insert Variable** button to insert one or more event variables into the message.

How To Create a Network Popup Notification Method

» To create a Network Popup Notification Method:

1. Right-click on the **Notification Methods** container in the ELM Console and select **All Tasks | New Notification Methods**. The **Create Notification Method Wizard** will appear. Click **Next** to continue.
2. Select **Network Popup** from the **Notification Method** dropdown and click **Next** to continue.
3. The Network Message Settings dialog box will appear.
 - In the **Computer** name field, enter the NetBIOS name of the computer to which you want the message sent. You can use the **Browse** button to browse your network for a computer.

- In the **Message** field, enter the message you want transmitted. You can completely customize the message. Use the **Insert Variable** button to insert one or more event variables into the message.
 - Use the **Test** button to test the Network Message Notification Method.
- 4. Click **Next** to continue. The **Rules** dialog box will appear. Put a checkmark next to each Rule you want to trigger this Notification Method. Click **Next** to continue.
- 5. The **Threshold** dialog box will appear. You can specify three different threshold settings:
 - a. **Disable this notification when it is triggered.** If the Notification Method is triggered the configured number of times within the specified time period, the notifications will stop. The Notification Method is then re-enabled after the time period specified.
 - b. **Activate this notification method after it is triggered.** When this threshold is selected, the notifications will not be processed unless the rule is triggered the specified number of times within the time period selected.
 - c. **Consolidate notifications by waiting until either.** You can configure the Notification Method to wait until being executed until either a specific number of similar events has occurred, or until a specific amount of time has elapsed.
- 6. If you don't want to be notified for cached data, check the box that says **Disable this notification method for all Cached (old) data**.
- 7. Click **Next** to continue. The **Schedule** dialog box will appear. Use your mouse to configure the hours and days you want this Notification Method active.
- 8. Click **Next** to continue. Enter a Name and Description and if desired, check the **Make this a default selection for new items** checkbox.
- 9. Click **Finish** to save the item.

Pagers

ELM supports both Numeric and Alpha-Numeric Pagers. You can send events to numeric, alphanumeric, TAP and SMS pagers using the Pager Notification Method and a modem attached to your ELM Server. To use this Notification Method, you must have an available modem connected to your ELM Server, and a pager service.

If your pager service can accept messages from a web page provided by your pager service provider, you may also be able to use the Web Post Notification Method.

How To Create a Pager Notification Method

» To create a Numeric Pager Notification Method:

1. Right-click on the **Notification Methods** container in the ELM Console and select **All Tasks | New Notification Method**. The **Create Notification Method Wizard** will appear. Click **Next** to continue.
2. Select **Pager Notification** from the dropdown and click **Next** to continue.
3. The Select Pager Type dialog box will appear. Select **Numeric Pager** from the dropdown. Click **Next** to continue.
4. The Connection Settings dialog box will appear. In the **Number of retries** field, enter in the number of times you want the ELM Server to try to page you. Using the **Pager Script** dropdown, select your pager or pager type. If you need to modify one of the included pager scripts, we recommend copying the script and making your modifications to the copy. Use the **Copy** button to copy a script. You can also use the **Edit** button to modify the script listed in the

Pager Script dropdown, and use the **Delete** button to delete the script listed in the **Pager Script** dropdown. Click the **New** button to create a new script from scratch.

5. Click **Next** to continue. The Account Numbers dialog box will appear. Enter your pager service account information:
 - **Name.** Enter a friendly name for the pager (e.g., Joe's Pager, or Help Desk Pager, etc.).
 - **Pager Number.** Enter the account number (also known as a PIN) for your pager service. If you do not have an account number or PIN, leave this field blank.
 - **Add account number to list.** Click this button to add the pager (name+PIN) to the Account Number List.
6. Click **Next** to continue. The Message dialog box will appear. Enter the numeric message you want sent to the pager in the **Numeric Message** field. Use the **Test** button to verify that your pager receives the intended message.
7. Click **Next** to continue. The **Rules** dialog box will appear. Put a checkmark next to each Rule you want to trigger this Notification Method. Click **Next** to continue.
8. The **Threshold** dialog box will appear. You can specify three different threshold settings:
 - a. **Disable this notification when it is triggered.** If the Notification Method is triggered the configured number of times within the specified time period, the notifications will stop. The Notification Method is then re-enabled after the time period specified.
 - b. **Activate this notification method after it is triggered.** When this threshold is selected, the notifications will not be processed unless the rule is triggered the specified number of times within the time period selected.
 - c. **Consolidate notifications by waiting until either.** You can configure the Notification Method to wait until being executed until either a specific number of similar events has occurred, or until a specific amount of time has elapsed.
9. If you don't want to be notified for cached data, check the box that says **Disable this notification method for all Cached (old) data**.
10. Click **Next** to continue. The **Schedule** dialog box will appear. Use your mouse to configure the hours and days you want this Notification Method active.
11. Click **Next** to continue. Enter a Name and Description and if desired, check the **Make this a default selection for new items** checkbox.
12. Click **Finish** to save the item, and click **OK** to acknowledge the item creation.

» To create an Alphanumeric Pager Notification Method:

1. Right-click on the **Notification Methods** container in the ELM Console and select **All Tasks | New Notification Methods**. The **Create Notification Method Wizard** will appear. Click **Next** to continue.
2. Select **Pager Notification** from the dropdown and click **Next** to continue.
3. The Select Pager Type dialog box will appear. Select **Alpha-Numeric Pager** from the dropdown. Click **Next** to continue.
4. The Connection Settings dialog box will appear. In the **Number of retries** field, enter in the number of times you want the ELM Server to try to page you. Using the **Pager Script** dropdown, select your pager or pager type. If you need to modify one of the included pager scripts, we recommend copying the script and making your modifications to the copy. Use the **Copy** button to copy a script. You can also use the **Edit** button to modify the script listed in the **Pager Script** dropdown, and use the **Delete** button to delete the script listed in the **Pager**

Script dropdown. Click the **New** button to create a new script from scratch.

5. Click **Next** to continue. The Account Numbers dialog box will appear. Enter your pager service account information:
 - **Name.** Enter a friendly name for the pager (e.g., Joe's Pager, or Help Desk Pager, etc.).
 - **Pager Number.** Enter the account number (also known as a PIN) for your pager service. If you do not have an account number or PIN, leave this field blank.
 - **Add account number to list.** Click this button to add the pager (name+PIN) to the Account Number List.
6. Click **Next** to continue. The Access Number dialog box will appear. Enter in the access phone number for your pager service in the **Pager Service Access Number** field. If you need to dial a number to get out, or dial a long distance number, be sure to add the appropriate leading characters to this string. For example, if you need to press 9 before dialing out, and your pager service is a 1-800 number, you would enter the number using the following format: **9, 18005551212**. In the **Message** field, enter the message you want transmitted to your pager. You can use the **Insert Variable** button to insert an event field as an environment variable in the message. Click the **Test** button to test and verify your pager settings and message reception.
7. Click **Next** to continue. The **Rules** dialog box will appear. Put a checkmark next to each Rule you want to trigger this Notification Method. Click **Next** to continue.
8. The **Threshold** dialog box will appear. You can specify three different threshold settings:
 - a. **Disable this notification when it is triggered.** If the Notification Method is triggered the configured number of times within the specified time period, the notifications will stop. The Notification Method is then re-enabled after the time period specified.
 - b. **Activate this notification method after it is triggered.** When this threshold is selected, the notifications will not be processed unless the rule is triggered the specified number of times within the time period selected.
 - c. **Consolidate notifications by waiting until either.** You can configure the Notification Method to wait until being executed until either a specific number of similar events has occurred, or until a specific amount of time has elapsed.
9. If you don't want to be notified for cached data, check the box that says **Disable this notification method for all Cached (old) data**.
10. Click **Next** to continue. The **Schedule** dialog box will appear. Use your mouse to configure the hours and days you want this Notification Method active.
11. Click **Next** to continue. Enter a Name and Description and if desired, check the **Make this a default selection for new items** checkbox.
12. Click **Finish** to save the item, and click **OK** to acknowledge the item creation.

SNMP Notification

ELM supports two different SNMP-based Notification Methods:

- The ELM Server includes an SNMP Trap Notification Method. It can take any alert, event or alarm and forward it as an SNMP trap to another ELM Server, or a customer owned SNMP management system.
- The ELM Server includes an SNMP OID Notification Method. It can take any valid SNMP Object ID (OID) and put (write) it to the specified target host or SNMP management system.

Note

In order to use either SNMP Notification Method, you must have the SNMP service installed on your ELM Server. The SNMP service is an optional component that comes with Windows NT, Windows 2000 and Windows XP. The SNMP service is also used to configure trap destinations.

After installing the SNMP service, you must configure the appropriate trap destinations via the operating system's SNMP configuration.

How To Create an SNMP Notification Method

The ELM Server includes an SNMP Trap notification method. It can take any alert, event or alarm and forward it as an SNMP trap to another ELM Server, or a customer owned SNMP management system.

In addition, the ELM Server also includes an SNMP OID notification method. It can take any valid SNMP Object ID (OID) and put (write) it to the specified target host or SNMP management system.

Note

By default, the SNMP OID Monitor and the SNMP OID Notification Method use a root of .1.3.6.1 of the SNMP OID tree. By adding the following registry value to the ELM Server, you can specify a different OID root:

Key: HKCU\Software\TNT
Software\<product>\<version>\Wizard\Settings\SnpRootOID
Value: ".1.3.x.y.z"
Type: String Value

Where: <product> is either ELM Performance Manager, ELM Log Manager or ELM Performance Manager
<version> is the product's major version (e.g., 3.0)
x.y.z is the root branch you want.

» To create an SNMP OID Notification Method:

1. Right-click on the **Notification Methods** container in the ELM Console and select **All Tasks | New Notification Methods**. The **Create Notification Method Wizard** will appear. Click **Next** to continue.
2. Select **SNMP OID Trap** from the **Notification Method** dropdown and click **Next** to continue.
3. The SNMP Notification settings dialog box will appear. Select **SNMP OID** from the dropdown. Click **Next** to continue.
4. The **OID Settings** dialog box will appear. If you do not want to specify the OID value, uncheck the **Set OID Value** checkbox, and click **Next** to continue and proceed to Step 5. If you do want to specify the OID, follow steps a-e.
 - a. To include a specific OID with this trap, make sure the **Set OID Value** checkbox is checked.
 - b. Next, enter the host and community name for a computer containing the OID whose value you want to set.
 - c. Next, click the **Display Objects from computer/community** button to read in the list of SNMP Objects and OIDs from this host/community.

- d. Select the OID you want to use, along with the condition and value you want to set for the selected OID. Note that you cannot change the Object Identifier field.
 - e. Set optional **Timeout** and **Retries** values.
 5. The **Trap Settings/Test** dialog box will appear. In order to send an SNMP Trap, the **Send SNMP Trap** checkbox must be checked. If this is a system trap, set the **Trap ID** and the **Enterprise ID**. For an event trap, check the box that says **Use Event ID for Trap ID** and enter the **Enterprise ID**. Click the **Test** button to test the notification method.
 6. Click **Next** to continue. The **Rules** dialog box will appear. Put a checkmark next to each Rule you want to trigger this Notification Method. Click **Next** to continue.
 7. The **Threshold** dialog box will appear. You can specify three different threshold settings:
 - a. **Disable this notification when it is triggered.** If the Notification Method is triggered the configured number of times within the specified time period, the notifications will stop. The Notification Method is then re-enabled after the time period specified.
 - b. **Activate this notification method after it is triggered.** When this threshold is selected, the notifications will not be processed unless the rule is triggered the specified number of times within the time period selected.
 - c. **Consolidate notifications by waiting until either.** You can configure the Notification Method to wait until being executed until either a specific number of similar events has occurred, or until a specific amount of time has elapsed.
 8. If you don't want to be notified for cached data, check the box that says **Disable this notification method for all Cached (old) data**.
 9. Click **Next** to continue. The **Schedule** dialog box will appear. Use your mouse to configure the hours and days you want this Notification Method active.
 10. Click **Next** to continue. Enter a Name and Description and if desired, check the **Make this a default selection for new items** checkbox.
 11. Click **Finish** to save the item.
- » To create an SNMP Trap Notification Method:
1. Right-click on the **Notification Methods** container in the ELM Console and select **All Tasks | New Notification Methods**. The **Create Notification Method Wizard** will appear. Click **Next** to continue.
 2. Select **SNMP OID Trap** from the **Notification Method** dropdown and click **Next** to continue.
 3. The SNMP Notification settings dialog box will appear. Select **SNMP Trap** from the dropdown. Click **Next** to continue.
 4. The Trap Settings/Test dialog box will appear. Configure the SNMP Trap settings as desired.
 - **Use Event ID as Trap ID.** Check this box if you want the event ID to be used as the trap ID.
 - **Trap ID.** If you don't want to use the event ID as the trap ID, uncheck the Use Event ID as Trap ID checkbox, and enter the ID number you want the trap to have in this field.
 - **Enterprise ID.** Use this field to specify an enterprise ID for the trap message.
 - Use the **Test** button to test the trap generation and settings.
 5. Click **Next** to continue. The **Rules** dialog box will appear. Put a checkmark next to each Rule you want to trigger this Notification Method. Click **Next** to continue.

6. The **Threshold** dialog box will appear. You can specify three different threshold settings:
 - a. **Disable this notification when it is triggered.** If the Notification Method is triggered the configured number of times within the specified time period, the notifications will stop. The Notification Method is then re-enabled after the time period specified.
 - b. **Activate this notification method after it is triggered.** When this threshold is selected, the notifications will not be processed unless the rule is triggered the specified number of times within the time period selected.
 - c. **Consolidate notifications by waiting until either.** You can configure the Notification Method to wait until being executed until either a specific number of similar events has occurred, or until a specific amount of time has elapsed.
7. If you don't want to be notified for cached data, check the box that says **Disable this notification method for all Cached (old) data**.
8. Click **Next** to continue. The **Schedule** dialog box will appear. Use your mouse to configure the hours and days you want this Notification Method active.
9. Click **Next** to continue. Enter a Name and Description and if desired, check the **Make this a default selection for new items** checkbox.
10. Click **Finish** to save the item.

How To Create an SNMP Trap Notification Method

The ELM Server includes an SNMP Trap notification method. It can take any alert, event or alarm and forward it as an SNMP trap to another ELM Server, or a customer owned SNMP management system.

» To create an SNMP Trap Notification Method:

1. Right-click on the **Notification Methods** container in the ELM Console and select **All Tasks | New Notification Methods**. The **Create Notification Method Wizard** will appear. Click **Next** to continue.
2. Select **SNMP OID Trap** from the **Notification Method** dropdown and click **Next** to continue.
3. The SNMP Notification settings dialog box will appear. Select **SNMP Trap** from the dropdown. Click **Next** to continue.
4. The Trap Settings/Test dialog box will appear. Configure the SNMP Trap settings as desired.
 - **Use Event ID as Trap ID.** Check this box if you want the event ID to be used as the trap ID.
 - **Trap ID.** If you don't want to use the event ID as the trap ID, uncheck the Use Event ID as Trap ID checkbox, and enter the ID number you want the trap to have in this field.
 - **Enterprise ID.** Use this field to specify an enterprise ID for the trap message.
 - Use the **Test** button to test the trap generation and settings.
5. Click **Next** to continue. The **Rules** dialog box will appear. Put a checkmark next to each Rule you want to trigger this Notification Method. Click **Next** to continue.
6. The **Threshold** dialog box will appear. You can specify three different threshold settings:
 - a. **Disable this notification when it is triggered.** If the Notification Method is triggered the configured number of times within the specified time period, the notifications will stop. The Notification Method is then re-enabled after the time period specified.
 - b. **Activate this notification method after it is triggered.** When this threshold is selected, the notifications will not be processed unless the rule is triggered the specified

number of times within the time period selected.

- c. **Consolidate notifications by waiting until either.** You can configure the Notification Method to wait until being executed until either a specific number of similar events has occurred, or until a specific amount of time has elapsed.
7. If you don't want to be notified for cached data, check the box that says **Disable this notification method for all Cached (old) data**.
8. Click **Next** to continue. The **Schedule** dialog box will appear. Use your mouse to configure the hours and days you want this Notification Method active.
9. Click **Next** to continue. Enter a Name and Description and if desired, check the **Make this a default selection for new items** checkbox.
10. Click **Finish** to save the item.

Sound File

Sound File Notification Methods are used to play a specific sound file (in .WAV format) on the ELM Server. The sound file notification message is executed on the computer running the ELM Server, and not by any Consoles that may be connected to the ELM Server. If the ELM Server does not have any sound system (e.g., sound card, speaker(s)), you will not be able to use the sound file Notification Method.

Note

When selecting the path and filename using an ELM Console installed on a computer other than the ELM Server, be aware of the following:

- The Browse button browses the local file system (e.g., the file system on the ELM Console computer), and not the file system on the ELM Server.
- If you do use the Browse button on a remote ELM Console to specify the path and filename for the sound file, the path and filename for the sound file must be identical on the ELM Console and ELM Server computers.
- If you know the path and filename local to the ELM Server, you can type that in the field.

How To Create a Sound File Notification Method

» To create a Sound File Notification Method:

1. Right-click on the **Notification Methods** container in the ELM Console and select **All Tasks | New Notification Method**.
2. The **Create Notification Method Wizard** will appear. Click **Next** to continue.
3. Select **Sound File** from the Notification Method dropdown and click **Next** to continue.
4. The **Sound File Settings** dialog box will appear.
 - Enter the path and filename to the sound file, or click the **Browse** button to search for the file you want to use.

- Use the **Volume Slider** to adjust the volume settings to the desired level. You can use the **Test** button to test the sound file.
5. Click **Next** to continue. The **Rules** dialog box will appear.
 6. Put a check mark next to each Rule to which you want this Notification Method applied.
 7. Click **Next** to continue. The **Threshold** dialog box will appear. You can specify three different threshold settings:
 - a. **Disable this notification when it is triggered.** If the Notification Method is triggered the configured number of times within the specified time period, the notifications will stop. The Notification Method is then re-enabled after the time period specified.
 - b. **Activate this notification method after it is triggered.** When this threshold is selected, the notifications will not be processed unless the rule is triggered the specified number of times within the time period selected.
 - c. **Consolidate notifications by waiting until either.** You can configure the Notification Method to wait until being executed until either a specific number of similar events has occurred, or until a specific amount of time has elapsed.
 8. If you don't want to be notified for cached data, check the box that says **Disable this notification method for all Cached (old) data**.
 9. Click **Next** to continue. The **Schedule** dialog box will appear. Use your mouse to configure the hours and days you want this Notification Method active.
 10. Click **Next** to continue. The **Name** dialog box will appear. Enter a meaningful name for the Notification Method, and an optional description. If you want this Notification Method to be automatically applied to all newly created Rules, check the box that says **Make this item a default selection for new items**.
 11. Click **Finish** to save this Notification Method. You will be prompted to create another Notification Method. Select **Yes** or **No** at your discretion.

Syslog Notification

The ELM Server includes a Syslog notification method that can be used to send events and alerts as Syslog messages to an upstream Syslog server or daemon. ELM supports both TCP and UDP-based Syslog notification.

How To Create a Syslog Notification Method

» To create a Syslog Notification Method:

1. Right-click on the **Notification Methods** container in the ELM Console and select **All Tasks | New Notification Methods**. The **Create Notification Method Wizard** will appear. Click **Next** to continue.
2. Select **Syslog Message** from the **Notification Method** dropdown and click **Next** to continue.
3. The Syslog Server Settings dialog box will appear.
 - Enter the host name, IP address or fully -qualified domain name of the Syslog server in the **Syslog Server Host Name** field.
 - In the **Port** field, select the port on which the Syslog server is listening. By default this port is TCP or UDP port 514.
 - In the **Sockets Type** field, select the protocol you want to use (TCP or UDP).

4. Click **Next** to continue. The Syslog Message dialog box will appear. Enter the message you want sent to the Syslog server when this notification method is executed. You can use the **Insert Variable** button to insert one or more event variables in the message. Click the **Test** button to test the Syslog notification method.
5. Click **Next** to continue. The **Rules** dialog box will appear. Put a checkmark next to each Rule you want to trigger this Notification Method. Click **Next** to continue.
6. The **Threshold** dialog box will appear. You can specify three different threshold settings:
 - a. **Disable this notification when it is triggered.** If the Notification Method is triggered the configured number of times within the specified time period, the notifications will stop. The Notification Method is then re-enabled after the time period specified.
 - b. **Activate this notification method after it is triggered.** When this threshold is selected, the notifications will not be processed unless the rule is triggered the specified number of times within the time period selected.
 - c. **Consolidate notifications by waiting until either.** You can configure the Notification Method to wait until being executed until either a specific number of similar events has occurred, or until a specific amount of time has elapsed.
7. If you don't want to be notified for cached data, check the box that says **Disable this notification method for all Cached (old) data**.
8. Click **Next** to continue. The **Schedule** dialog box will appear. Use your mouse to configure the hours and days you want this Notification Method active.
9. Click **Next** to continue. Enter a Name and Description and if desired, check the **Make this a default selection for new items** checkbox.
10. Click **Finish** to save the item.

Text-To-Speech Notification

You can have any event read by an electronic voice on the ELM Server. The speech-to-text engine allows you to choose a synthesized human voice that speaks the message that is passed to it. You can pass the event unmodified, or customize it to suit your needs.

Note

The notification message is spoken by the computer running the ELM Server, and not by any Consoles that may be connected to the ELM Server. If the ELM Server does not have any sound system (e.g., sound card, speaker(s)), you will not be able to use the speech Notification Method. In addition, you must install the [Microsoft Speech SDK 5.0](#) or later in order to use this Notification Method.

How To Create a Text-to-Speech Notification Method

» To create a Text-to-Speech Notification Method:

1. Right-click on the **Notification Methods** container in the ELM Console and select **All Tasks | New Notification Methods**. The **Create Notification Method Wizard** will appear. Click **Next** to continue.

2. Select **Text-to-Speech** from the **Notification Method** dropdown and click **Next** to continue.
3. The Speech Settings dialog box will appear.
 - In the **Speech Voice** dropdown, select the voice you want to use.
 - In the **Message** field, enter the message you want said when this Notification Method is executed. You can use the **Insert Variable** button to insert an event field as an environment variable in the the message (e.g., %computer%, %type%, etc.).
 - Enter the number of times you want the message spoken in the **Repeat message ___ times** field.
 - Click the **Test** button to test the speech Notification Method. The ELM Server will speak the message in the **Message** field.
4. Click **Next** to continue. The **Rules** dialog box will appear. Put a checkmark next to each Rule you want to trigger this Notification Method. Click **Next** to continue.
5. The **Threshold** dialog box will appear. You can specify three different threshold settings:
 - a. **Disable this notification when it is triggered.** If the Notification Method is triggered the configured number of times within the specified time period, the notifications will stop. The Notification Method is then re-enabled after the time period specified.
 - b. **Activate this notification method after it is triggered.** When this threshold is selected, the notifications will not be processed unless the rule is triggered the specified number of times within the time period selected.
 - c. **Consolidate notifications by waiting until either.** You can configure the Notification Method to wait until being executed until either a specific number of similar events has occurred, or until a specific amount of time has elapsed.
6. If you don't want to be notified for cached data, check the box that says **Disable this notification method for all Cached (old) data**.
7. Click **Next** to continue. The **Schedule** dialog box will appear. Use your mouse to configure the hours and days you want this Notification Method active.
8. Click **Next** to continue. Enter a Name and Description and if desired, check the **Make this a default selection for new items** checkbox.
9. Click **Finish** to save the item, and click **OK** to acknowledge the item creation.

Web Post Notification

ELM supports the posting of a form to an internal or external Web site as a notification method. This is especially useful in intranets, as well as for alphanumeric pagers. Note that ELM provides the posting capabilities only; it does not include any Web forms that can be used for posting. However, by using Microsoft FrontPage or similar Web authoring tool, you can easily create Web forms for your intranet.

The information contained in the event is available to the Web Post method through environment variables, enabling you to send the event as is, or to customize it to your liking.

How To Create a Web Post Notification Method

» To create a Web Post Notification Method:

1. Right-click on the **Notification Methods** container in the ELM Console and select **All Tasks | New Notification Methods**. The **Create Notification Method Wizard** will appear. Click **Next**

to continue.

2. Select **Post Web Page** from the **Notification Method** dropdown and click **Next** to continue.
3. The **Web Site Options** dialog box will appear.
 - If the web site you want to post to requires authentication, check the **Use Logon Credentials** checkbox and enter a valid **Username** and **Password**.
 - In the **Keywords** section, you can enter Success and/or Failure Keywords. The resulting Web page will then be searched for the specified keywords to more accurately determine whether or not the Web Post Notification Method was successful.
4. Click **Next** to continue. Enter the **URL** for the web form you want to use for posting in the Web Form URL field. The page will be displayed in the field below. Fill out all required and any optional fields in this form. Click the **Copy** button to insert one or more event variables into a field.
5. Click the **Test** button to test the notification method.
6. Click **Next** to continue.
7. The **Rules** dialog box will appear. Put a checkmark next to each Rule you want to trigger this Notification Method. Click **Next** to continue.
8. The **Threshold** dialog box will appear. You can specify three different threshold settings:
 - a. **Disable this notification when it is triggered.** If the Notification Method is triggered the configured number of times within the specified time period, the notifications will stop. The Notification Method is then re-enabled after the time period specified.
 - b. **Activate this notification method after it is triggered.** When this threshold is selected, the notifications will not be processed unless the rule is triggered the specified number of times within the time period selected.
 - c. **Consolidate notifications by waiting until either.** You can configure the Notification Method to wait until being executed until either a specific number of similar events has occurred, or until a specific amount of time has elapsed.
9. If you don't want to be notified for cached data, check the box that says **Disable this notification method for all Cached (old) data**.
10. Click **Next** to continue. The **Schedule** dialog box will appear. Use your mouse to configure the hours and days you want this Notification Method active.
11. Click **Next** to continue. Enter a Name and Description and if desired, check the **Make this a default selection for new items** checkbox.
12. Click **Finish** to save the item, and click **OK** to acknowledge the item creation.

Rules

Rules are used to trigger one or more actions when an Alert occurs. Rules tie together your Event Filters and Notification Methods. You can specify that an Alert must match all selected filters before it triggers a rule. This means that you can use multiple filters in tandem to trigger (or not trigger) Rules. To specify that an Alert must match all selected filters before the rule is applied, select the option that says Events must match all selected filters to be included.

Alternatively, if you want the Rule to be triggered if any one of the selected filters are matched, select the option that says Events matching at least one selected filter will be included.

How To Create a Rule

» To create a new Rule:

1. Right-click on the **Rules** object in the ELM Console, and select **All Tasks | New Rule**. This will launch the **Notification Rule Wizard**. Click **Next** to continue.
2. The **Notification Rule Settings** dialog box will appear. Select one of the options:
 - a. **Events must match all selected filters to be included**. If this is selected, only events that match all of the selected filters will cause this Rule to trigger the selected Notification Method(s).
 - b. **Events matching at least one selected filter will be included**. If this is selected, events that match any of the selected filters will cause this Rule to trigger the selected Notification Method(s).
3. Click **Next** to continue. The **Select Filters** dialog box will appear. Put a checkmark next to the Filter(s) you want to associate with this Rule. You can also create a new Filter from this dialog by right-clicking anywhere and selecting **New Select Event Filter**. In addition, you can view the properties of any Event Filter by right-clicking on the Filter and selecting **Properties**.
4. Click **Next** to continue. The **Select Exclude Filters** dialog box will appear. Put a checkmark next to the Exclude Filter(s) you want to associate with this Rule. You can also create a new Exclude Filter from this dialog by right-clicking anywhere and selecting **New Select Exclude Filter**. In addition, you can view the properties of any Exclude Filter by right-clicking on the Filter and selecting **Properties**.
5. Click **Next** to continue. The **Select Notification Methods** dialog box will appear. Put a checkmark next to the Notification Method(s) you want to be triggered by this Rule. You can also create a new Notification Method from this dialog by right-clicking anywhere and selecting **New Select Notification Method**. In addition, you can view the properties of any Notification Method by right-clicking on the Notification Method and selecting **Properties**.
6. Click **Next** to continue. Provide the filter with a meaningful name and an optional description.
7. Click **Finish** to save the Rule.

Rules can also be created from Alerts.

» To create a new Rule from an Alert:

1. Right-click on any Alert and select **All Tasks | New Rule**.
2. This will launch the **Notification Rule Wizard**. Click **Next** to continue.
3. The **Notification Rule Settings** dialog box will appear. Select one of the options:
 - a. **Events must match all selected filters to be included**. If this is selected, only events that match all of the selected filters will cause this Rule to trigger the selected Notification Method(s).
 - b. **Events matching at least one selected filter will be included**. If this is selected, events that match any of the selected filters will cause this Rule to trigger the selected Notification Method(s).
4. Click **Next** to continue. The **Select Filters** dialog box will appear. At the top of the list is a selected Event Filter that was automatically created based on some of the event criteria in the event or alert used in Step 1. **Double-click** the Event Filter to view its

criteria and verify that you want to use the auto-populated criteria.

5. Click **Next** to continue. The **Select Exclude Filters** dialog box will appear. Put a checkmark next to the Exclude Filter(s) you want to associate with this Rule. You can also create a new Exclude Filter from this dialog by right-clicking anywhere and selecting **New Select Exclude Filter**. In addition, you can view the properties of any Exclude Filter by right-clicking on the Filter and selecting **Properties**.
6. Click **Next** to continue. The **Select Notification Methods** dialog box will appear. Put a checkmark next to the Notification Method(s) you want to be triggered by this Rule. You can also create a new Notification Method from this dialog by right-clicking anywhere and selecting **New Select Notification Method**. In addition, you can view the properties of any Notification Method by right-clicking on the Notification Method and selecting **Properties**.
7. Click **Next** to continue. Provide the filter with a meaningful name and an optional description.
8. Click **Finish** to save the Rule.

Reports

Creating reports from collected data

ELM includes a robust reporting engine that enables administrators to create, edit and schedule reports without requiring any additional software.

All reports are stored in the Reports container. This container, as well as individual reports, support the application of Windows Access Control Lists (ACLs). You can secure the entire container, or secure individual reports.

You can create reports containing data from any table in the ELM Server database, including:

- Alerts, which are stored in a table called **TNTAlerts**.
- Performance Data, which is stored in tables whose names begin with PD (e.g., **PDMemory**).

Reports can also be scheduled to run automatically at periodic intervals. There are a variety of report formats to choose from:

- Printer
- Screen (cannot be used for scheduled reports)
- Native File
- Rich Text
- HTML
- ASCII Text
- Ask When Run (cannot be used for scheduled reports)
- Comma Delimited
- Tab Delimited

Notes

ELM comes pre-populated with several reports. These reports are sample reports that are ready for use. However, they may require additional formatting or reformatting to compensate for long Alerts or Alerts with unusual formatting. The height and width of the message details field and the placement of the vertical line are based on average sized event records. If you have event records with lengthy message text, you will need to enlarge the Detail Section, move the vertical line down toward the bottom of the Detail Section, and increase the height and width of the Message field.

Some reports are wide enough that they require landscape format in order to fit everything on the page. In order to do this, you must have a default printer installed on the ELM Server, even if you do not plan on printing reports. Having a default printer is the only way ELM can programmatically manipulate the page orientation from portrait to landscape.

How To Create Reports

ELM includes a built-in report engine that enables administrators to create reports without installing any additional software. Reports can be produced on a scheduled basis in a variety of formats (e.g., HTML, Rich-Text Format, ASCII), or sent to a printer.

» To Create a New report:

1. Right-click on the Reports container and select **All Tasks | New Report**. The Create New Report Wizard will start. Click **Next** to continue.
2. The Name dialog box will appear. Enter a **Name** for the report along with an optional **Description**. Click **Next** to continue.
3. The Tables dialog box will appear. Use this dialog box to include tables from your database in this report.
 - Select the table or tables you want included in the **Tables in Database** field.

Note

If you want to include all of the fields, simply click the Add All button.

- Click the **Add** button to add them to the **Tables available for Report** field.
 - You can use the **Remove** or **Remove All** button to move tables from the **Tables available for Report** field back to the **Tables in Database** field.
4. Click **Next** to continue. The Select Fields dialog box will appear. Use this dialog to select the fields you want included in this report.
 - Select the table or tables you want included in the list of **Available Fields**.

Note

If you want to include all of the fields, simply click the Add All button. **Tip: If you are creating a report from a database with a large number of records, don't select any fields here; instead, put them in the summarize fields.**

- Click the **Add** button to add the selected field(s) to the **Fields to Display** field. Use the **Add All** button to add all available fields to the report.
- You can use the **Remove** or **Remove All** button to move fields from the **Fields to Display** field back to the list of **Available Fields**.
- When selecting a field from the Available Fields, you can use the **Field Data** button to browse the data in the selected field. You can also use the **Find Field** button to search for a specific field.

- When a field is selected in the **Fields to Display** field, the report heading for that field will be displayed in the **Heading** field. If desired, you can modify this heading to display something other than the default.
5. Click **Next** to continue. The Summarize dialog box will appear. If you expect the report you are creating to be long, you may find it useful to group information in the report at the field level. Summarizing report fields, also known as grouping, is essentially the same as sorting them.
- Use the **Add** button to add a field from the **Available Fields** field to the **Group By** field.
 - Use the **Remove** or **Remove All** button to remove one, some or all fields from the **Group By** field.
 - When selecting a field from the Available Fields, you can use the **Field Data** button to browse the data in the selected field. You can also use the **Find Field** button to search for a specific field.
 - Use the **Sort Order** dropdown to sort the report in ascending or descending format.
6. Click **Next** to continue. The Select Filter Criteria dialog box will appear. Use this dialog to customize the SQL query used in the report. This is done through the use of filters. Filters are used in SQL WHERE statements.
- To add a filter: Select a column in the **Available Fields** field. Select a condition from the **Is** dropdown. Enter a value in the **Value** field. Click the **Add** button to add the conditional statement to the **Filters** field.
 - To add additional filters: Select a column in the **Available Fields** field. Select a condition from the **Is** dropdown. Enter a value in the **Value** field. Select an operator (**AND** or **OR**). Click the **Add** button to add the conditional statement to the **Filters** field. Repeat these steps for each additional filter you want to add.

Note

If your filter includes a LIKE statement, make sure one of the following formats is used: %SERVERA%, or %SERVERA, or SERVERA%, depending on your desired match. You can modify existing a report's existing SQL statement through the Report Properties dialog.

- To modify an existing filter: Select the filter in the **Filters** field. Use the **Is**, **Value** and operator (**AND** or **OR**) fields to modify the filter criteria. Click the **Update** button.
 - Use the **Remove** or **Remove All** button to remove one or all filters from the **Filters** field.
7. Click **Next** to continue. The Chart Type dialog box will appear. If applicable, select the type of Chart you want to use. If you select a chart type, a dialog will appear in the Wizard that will allow you to specify the chart's appearance (e.g., colors, fonts, legend, data values, etc).

Note

When creating a stacked bar chart, you must enter two fields in the *On Change Of* section, and one field in the *Show Values* section. If you do not choose the proper number and types of fields, you will not be able to complete the Chart Wizard.

8. Click **Next** to continue. The Output dialog box will appear. Select an **Output format** that can be scheduled:
- Native File

- Rich-Text
- HTML
- ASCII text
- Comma delimited
- Tab delimited

Then, specify the output path for the report.

9. Click **Next** to continue. The Schedule dialog box will appear. Use this dialog to schedule the report to run automatically.
 - In the **Every** field, change the interval to something other than NEVER. You can specify interval increments of minutes, hours, days, weeks, months and quarters.
 - Using the **Calendar control**, select the date on which you want the schedule to start.
 - In the **Time** field, enter the time at which you want this report to be run for the first time.
10. Click **Next** to continue. The Actions dialog box will appear. Use this dialog to take action or generate notification when a scheduled report successfully runs, and/or when a scheduled report fails to run. There are two tabs: Failure and Success that you can configure with one or more of the following options:
 - **Create New Alert Entry.** Selecting this checkbox to cause an Alert to be generated and posted to the Alerts container within the Console snap-in.
 - **Create Application Event Log Entry.** Selecting this enables you to cause a customizable event to be logged to the Application log on the ELM Server. Use the **Variables** button to specify any additional variables you want the event to include.
 - **Net Send Message.** Using this option enables you to send a popup message over the network. The target system must have the Messenger Service (Windows NT, Windows 2000, or Windows XP) or WinPopUp (Win9x/WinMe) running in order to receive the Net Send Message. Use the **Browse** button to browse for a target computer, or manually enter the name of the computer to which you want to send messages in the **Computer Name** field.
 - **Run Command.** This option provides a mechanism for executing a batch file, running a command line application or launching a script. Use the **Edit** button to create and edit any scripts or command line parameters you want to execute.
11. Click **Finish** to save the Report.

How To Schedule Reports

ELM includes a built-in scheduler feature that enables administrators to run reports at periodic intervals. Reports can be produced on a scheduled basis in a variety of formats (e.g., HTML, Rich-Text Format, ASCII), or sent to a printer.

» To schedule a New report:

1. Right-click on the Reports container and select **All Tasks | New Report**. The Create New Report Wizard will start. Click **Next** to continue.
2. The Name dialog box will appear. Enter a **Name** for the report along with an optional **Description**. Click **Next** to continue.

3. The Tables dialog box will appear. Use this dialog box to include tables from your database in this report.

- Select the table or tables you want included in the **Tables in Database** field.

Note

If you want to include all of the fields, simply click the Add All button.

- Click the **Add** button to add them to the **Tables available for Report** field.
- You can use the **Remove** or **Remove All** button to move tables from the **Tables available for Report** field back to the **Tables in Database** field.

4. Click **Next** to continue. The Select Fields dialog box will appear. Use this dialog to select the fields you want included in this report.

- Select the table or tables you want included in the list of **Available Fields**.

Note

If you want to include all of the fields, simply click the Add All button.

- Click the **Add** button to add the selected field(s) to the **Fields to Display** field. Use the **Add All** button to add all available fields to the report.
- You can use the **Remove** or **Remove All** button to move fields from the **Fields to Display** field back to the list of **Available Fields**.
- When selecting a field from the Available Fields, you can use the **Field Data** button to browse the data in the selected field. You can also use the **Find Field** button to search for a specific field.
- When a field is selected in the **Fields to Display** field, the report heading for that field will be displayed in the **Heading** field. If desired, you can modify this heading to display something other than the default.

5. Click **Next** to continue. The Summarize dialog box will appear. If you expect the report you are creating to be long, you may find it useful to group information in the report at the field level. Summarizing report fields, also known as grouping, is essentially the same as sorting them.

- Use the **Add** button to add a field from the **Available Fields** field to the **Group By** field.
- Use the **Remove** or **Remove All** button to remove one, some or all fields from the **Group By** field.
- When selecting a field from the Available Fields, you can use the **Field Data** button to browse the data in the selected field. You can also use the **Find Field** button to search for a specific field.
- Use the **Sort Order** dropdown to sort the report in ascending or descending format.

6. Click **Next** to continue. The Select Filter Criteria dialog box will appear. Use this dialog to customize the SQL query used in the report. This is done through the use of filters. Filters are used in SQL WHERE statements.

- To add a filter: Select a column in the **Available Fields** field. Select a condition from the **Is** dropdown. Enter a value in the **Value** field. Click the **Add** button to add the conditional statement to the **Filters** field.
- To add additional filters: Select a column in the **Available Fields** field. Select a condition from the **Is** dropdown. Enter a value in the **Value** field. Select an operator

(**AND** or **OR**). Click the **Add** button to add the conditional statement to the **Filters** field. Repeat these steps for each additional filter you want to add.

- To modify an existing filter: Select the filter in the **Filters** field. Use the **Is**, **Value** and operator (**AND** or **OR**) fields to modify the filter criteria. Click the **Update** button.
 - Use the **Remove** or **Remove All** button to remove one or all filters from the **Filters** field.
7. Click **Next** to continue. The Chart Type dialog box will appear. If applicable, select the type of Chart you want to use. If you select a chart type, a dialog will appear in the Wizard that will allow you to specify the chart's appearance (e.g., colors, fonts, legend, data values, etc).
8. Click **Next** to continue. The Output dialog box will appear. Select an **Output format** that can be scheduled:
- Native File
 - Rich-Text
 - HTML
 - ASCII text
 - Comma delimited
 - Tab delimited

Then, specify the output path for the report.

9. Click **Next** to continue. The Schedule dialog box will appear. Use this dialog to schedule the report to run automatically.
- In the **Every** field, change the interval to something other than NEVER. You can specify interval increments of minutes, hours, days, weeks, months and quarters.
 - Using the **Calendar control**, select the date on which you want the schedule to start.
 - In the **Time** field, enter the time at which you want this report to be run for the first time.
10. Click **Next** to continue. The Actions dialog box will appear. Use this dialog to take action or generate notification when a scheduled report successfully runs, and/or when a scheduled report fails to run. There are two tabs: Failure and Success that you can configure with one or more of the following options:
- **Create New Alert Entry**. Selecting this checkbox to cause an Alert to be generated and posted to the Alerts container within the Console snap-in.
 - **Create Application Event Log Entry**. Selecting this enables you to cause a customizable event to be logged to the Application log on the ELM Server. Use the **Variables** button to specify any additional variables you want the event to include.
 - **Net Send Message**. Using this option enables you to send a popup message over the network. The target system must have the Messenger Service (Windows NT, Windows 2000, Windows 2003 or Windows XP) or WinPopUp (Win9x/WinMe) running in order to receive the Net Send Message. Use the **Browse** button to browse for a target computer, or manually enter the name of the computer to which you want to send messages in the **Computer Name** field.
 - **Run Command**. This option provides a mechanism for executing a batch file, running a command line application or launching a script. Use the **Edit** button to create and edit any scripts or command line parameters you want to execute.
11. Click **Finish** to save the Report.

» **To schedule (or modify the schedule of) an Existing report:**

1. Right-click the report whose schedule you want to add or modify, and select **Properties**.
2. From the **File** menu, choose **Report Properties**. Navigate to the **Schedule** tab. Use this dialog to schedule the report to run automatically.
 - In the **Every** field, change the interval to something other than NEVER. You can specify interval increments of minutes, hours, days, weeks, months and quarters.
 - Using the **Calendar control**, select the date on which you want the schedule to start.
 - In the **Time** field, enter the time at which you want this report to be run for the first time.
 - Click **OK** to save your changes.
3. Close the Report to save the schedule changes within the report. If prompted, say **Yes** to saving your changes.

How To Add a Chart to a Report

ELM includes the following types of charts that you can add to your reports:

- Side-by-side bar chart
- Stacked bar chart
- Pie chart
- Line chart

Charts can only be placed in the Report Header or Report Footer sections of a report. If your existing report does not have these sections, you will need to first add one before creating and adding the chart. Select **Section** from the **Insert** menu in the report editor to add a Report Header or Report Footer section.

» **To add a chart to a report:**

1. Open the report to which you want to add a chart. You can do this by double-clicking the report in the Reports container.
2. From the Report Editor menu, select **Insert**, then select **Chart**. The Chart Wizard will launch.
3. You can select from the following chart types:
 - None (No chart will be included in the report)
 - Line chart
 - Side-by-side bar chart
 - Stacked bar chart
 - Pie chart

Note

When creating a stacked bar chart, you must enter two fields in the *On Change Of* section, and one field in the *Show Values* section. If you do not choose the proper number and types of fields, you will not be able to complete the Chart Wizard.

4. Select a chart type and click Next to continue. The Chart Data screen will appear. Enter the fields you want represented in the chart.

- Use the **Place** field to specify whether you want the selected data to be in the Header or Footer of the chart.
 - Select an **Available Field** and use the top **Add** button to add the field to the **On Change Of** field. Use the **Time** dropdown to specify the interval you want to use for the field you are using in the **On Change Of** field.
 - Select one or more field from **Available Fields** and click the lower **Add** button to add the field to the **Show Values** field.
 - When selecting a field from the Available Fields, you can use the **Field Data** button to browse the data in the selected field. You can also use the **Find Field** button to search for a specific field.
 - If you want to change how the field data is summarized, use the **Summary Type** dropdown to specify a method (e.g., Sum, Average, Count, Minimum or Maximum).
 - Use the **Matches** field to only show chart data that matches the value you specify here.
5. Click Next to continue. The Chart Options screen will appear. Use this dialog box to specify the options for this chart:
- **Show Legend.** By default, this box is checked and a legend for the chart will be displayed. If you do not want a chart legend displayed, uncheck this box.
 - **Show Values.** By default, this box is not checked and specific data values will not be displayed on the chart. If you want the specific data values shown on the chart, check this box.
 - **Auto Range.** If you want the chart range (e.g., chart low to chart high) to be automatically generated by the values corresponding to the chart's data, leave this box checked. For example, if you are charting % Processor Time and your data has values that range from 5% to 90%, then your range for data shown in the chart will start at 5% and end at 90%. If you want to specify your own range, uncheck this box, and enter the values you want to use in the **Minimum** and **Maximum** fields.
 - **Format Label.** This field is used to format the value of a label. This is particularly useful for labels whose values are very large (e.g., 1,000,000) and whose range is very small (e.g., 1-10). For example, you could use a label of 1M to represent 1,000,000. Use the **Applies To** dropdown to specify whether the format label should be applied to all data, or just the last value on the data axis.
 - **Title.** Use this dropdown to specify a Title for the chart.
 - **Text.** Use this field to specify the text you want to use for the title of the chart. Use the **Font** button to specify the font you want to use.
6. Click Finish to save the chart settings and close the Chart Wizard.
7. The chart will appear as an empty square. Use the arrow keys on the keyboard or your mouse to move the chart to the desired location. Note that a chart can only be placed in a report header or footer section. If you try to place a chart elsewhere, a warning dialog regarding this will be displayed.

Web Viewer

Using the Web-Based UI for ELM

The Web Viewer provides a read-only view of your ELM Server data. In addition to viewing information, you can also enable and disable items, and view reports that have been saved and output in HTML format.

If IIS is installed on your ELM Server, during installation of the ELM Server you are presented with an option to automatically create an ELM virtual directory on the ELM Server. If your IIS server is running multiple Web Sites (also known as Virtual Web Servers), you can select which Web Site you want to contain the ELM virtual directory. The virtual directory should point to the WebSite directory on your ELM Server (by default, C:\Program Files\TNT Software\ELM Performance Manager 3.1\WebSite).

The Web Viewer provides access to the following items:

- Agents
- Alerts
- Event Filters
- Notification Methods
- Reports
- Rules

The Web Viewer is implemented as a set of COM objects within Active Server Pages (ASP) documents. It uses the Extensible Markup Language (XML) as the transport mechanism for the data, making it lightweight and fast, and XSL (XML Styles) to format the data's appearance.

The Web Viewer can be installed on Internet Information Server/Services 5.0, 5.1 and 6.0. Integration with IIS means that you can secure the Web Viewer from unauthorized use. In addition, you can control the name of the virtual directory, the port, and other properties. The Web Viewer server components must run on the ELM Server computer.

Once installed on the server, you can access the Web Viewer by pointing your Web browser at the virtual directory (by default EPM31). For example, to access the Web Viewer on a server names SERVERA, you would point your Web browser to **http://servera/epm31**.

Note

While we recommend using Internet Explorer as your Web browser, the Web Viewer can be access using any Web browser that supports XML parsing and Javascript.

Web Viewer Security

You can secure the Web Viewer against unauthorized usage or access. You can secure Web Viewer access in two primary ways:

- **Securing IIS.** Microsoft has a security checklist [Internet Information Services 5.0](#). This document should be carefully reviewed, and steps should be taken to secure this IIS server.
- **Securing Containers and Items in the ELM Console.** You can use native Windows access control lists (ACLs) to secure containers or individual items.

Web Viewer User Interface

Once installed on the server, you can access the Web Viewer by pointing your Web browser at the virtual directory created during setup. The default name of the virtual directory for ELM Performance Manager is **epm31**.

As you might expect, the Web Viewer presents ELM Server and Agent data within a Web site. The hierarchy and presentation is very similar to what is shown in the ELM Console. On the left-hand side is the navigation menu. When you click one of the menu options on the left, the resulting page will be shown in the larger right-hand frame. There are several menu items on the left-hand side (which are duplicated with icons on the Web Viewer home page as shown above):

- **Agents.** This item takes you to the Agent Manager where you can view Agent Categories, and to a list of all Agents.
- **Alerts.** This displays the Alerts from the Alerts container. When viewing Alerts, you can view the details of an individual Alert by clicking on the icon to the left of the Alert message.
- **Event Filters.** This displays a list of all Event Filters. Clicking on an individual Event Filter will display that filter's properties.
- **Monitor Items.** This displays all Monitor Items, both enabled and disabled. Clicking on an individual Monitor Item allows you to enable and/or disable it.
- **Notification Methods.** This displays all Notification Methods. Clicking on an individual Notification Method enables you to drill down into it, where you can view its properties and its schedule.
- **Reports.** This displays a list of all Reports. Clicking on an individual Report enables you to view its properties. When displaying an individual report's properties, you can click on Preview Report to view a preview of the report.
- **Rules.** This displays a list of all Rules. Clicking on an individual Rule enables you to view its properties, as well as view the Event Filters and Notification Methods associated with the Rule.
- **Reports Folder.** This provides a directory browse of the output folder for Reports. Click on an individual report to view it.
- **Help.** Click on this link to download the compiled HTML Help file (.CHM file) which contains the ELM product documentation.
- **Read me.** Click on this link to download the Read Me file (in RTF format).

When viewing certain items, a second menu will appear on the right-hand side of the Web page that contains a variety of menu options:

- **Properties.** Click Properties to view the current item's properties.
- **Disable/Enable.** Where appropriate, you can enable and disable individual items from the Web Viewer. When an item is enabled, the Menu Option will read Disable. When the item is disabled, the Menu Option will read Enable.
- **Show Processes.** When viewing an Agent, you can click on Show Processes to view the list of current processes on the Agent system, along with per-process performance data. When viewing a specific process, a menu item for 'Kill Process' will be added to the menu shown above.
- **Show Services.** When viewing an Agent, you can click on Show Services to view the list of services that are installed on this Agent. When viewing a specific service, a menu item for **Start**, **Stop**, or **Pause** (depending on the service's current state) will be added to the menu shown above.
- **Show Devices.** When viewing an Agent, you can click on Show Devices to view the list of devices that are installed on this Agent. When viewing a specific service, a menu item for **Start**, **Stop**, or **Pause** (depending on the device's current state) will be added to the menu shown above.
- **Preview Report.** When viewing an individual report, you can display a preview of the report by clicking Preview Report.
- **Run Report.** When viewing an individual report, you can generate a report by clicking Run Report. Note that if the output format for the report is not set to HTML, you cannot run the report from the Web Viewer.

Pre-Configured Items

ELM Performance Manager includes several pre-configured items, many of which are ready for immediate use. The table below lists the pre-configured items and their purposes. The pre-configured items are there to provide some functionality out of the box, and to provide examples of how to configure various things. You do not need to use pre-configured items. You are free to modify and/or delete them and create your own objects and items.

Items are stored in the various containers that are shown in the left-hand (scope) pane of the ELM Console. Some items are set as a default, which means that they are automatically applied to any associated new items that get created. For example, the Ping Monitor is set as a default item. This means that every time you add a new Agent, the Ping Monitor will be automatically assigned to the new Agent. Finally, some items are enabled and some are disabled.

The table below details the pre-configured items that ship with ELM Performance Manager, including container location, whether or not the item is set as a default, and (where applicable) whether or not the item is enabled.

Container	Item Type	Name	Description	Default Selection	Enabled
Event Filters	Event Filter	All	All events from all event logs on all monitored Windows Agents	No	N / A
		ELM Agent Events	All events with a source of TNTAgent	No	
		ELM Agent Monitor Messages	All events generated by the Agent Monitor	No	
		ELM Monitor Errors	All errors or failures generated by an ELM Server or ELM Agent component	No	
		ELM Monitor Messages	All events generated by any Monitor Item	No	
		ELM Performance Alarm Messages	All events generated by the Performance Alarm	No	
		ELM Process	All events generated by the	No	

	Monitor Messages	Process Monitor		
	ELM Server Events	All events generated by an ELM Server	No	
	ELM WMI Monitor Messages	All events generated by the WMI Monitor	No	
	Errors	All error events	No	
	Informational	All information events	No	
	Warnings	All warning events	No	

Monitor Items	Agent Monitor	Agent Monitor	Performs 'heartbeat' check on Service Agent every 10 minutes. Also checks for QoS response time of 10 seconds or less and restarts TNT Agent service if service is stopped	Yes	Yes
	Performance Alarm	Percent Free Disk Space <= 5 %	Monitors to the LogicalDisk / % Free Disk Space counter every 15 minutes and generates an Alert when there is 5 % or less of the total disk space free	No	No
		Available Memory <= 20MB	Monitors the Memory / Available MBytes counter every 15 minutes and generates an Alert when the amount of free memory in megabytes is 20 or less	No	No
		Disk Queue Length >= 3	Monitors the LogicalDisk / Avg. Disk Queue Length counter for all logical disks every 15 minutes and generates an Alert of the value is 3 or greater	No	No
	Performance Data Collection Set	Windows NT/2000/XP Disk	Collects all LogicalDisk and PhysicalDisk performance objects/counters every 30 minutes	No	No
		Windows NT/2000/XP Memory	Collects all Memory and Paging File performance objects/counters every 30 minutes	No	No
		Windows NT/2000/XP Networking	Collects all Network Interface, ICMP, NBT, Network Segment, UDP, TCP and IP performance objects/counters every 30 minutes	No	No
		Windows	Collects all Process and	No	No

		NT/2000/XP Processes	Processor performance objects/counters every 30 minutes		
		Windows NT/2000/XP System	Collects all System performance objects/counters every 30 minutes	No	No
	Process Monitor	Process Monitor	Inspect all processes except _Idle and _Total every 30 minutes for excessive CPU utilization. Generates warning Alert when CPU usage by any process exceeds 50 % and error Alert when CPU usage exceeds 75 %	Yes	Yes

Notification Methods	Alert	Generate an Alert	Generates an Alert event in the Alerts container within the ELM Console	No	No
	Beep	Error Beep	Play a beep noise on the ELM Server computer when an error event is received	No	Yes
		Warning Beep	Play a beep noise on the ELM Server computer when a warning event is received	No	Yes
	Mail	Sample Send SMTP Mail	An example of how to send an SMTP mail message for notification purposes	No	No
	Network Pop-up Message	Sample Network Pop-up Message	An example of how to send a network message to a Windows computer for notification purposes	No	No
	Play Sound File	Sample Play Foghorn Sound File	An example of how to play a WAV sound file on the ELM Server for notification purposes	No	No
	Post Web Form	Sample Post Web Form to PageNet	An example of how to use a web post form to send a message to a PageNet Nationwide Pager service subscriber	No	No
	SNMP	Sample Send SNMP Trap	An example of how to send an SNMP Trap to any SNMP-capable management system (including an ELM Server) for notification purposes	No	No
	Syslog	Sample Send Syslog Message	An example of how to send a Syslog message to any Syslog Server (including an ELM Server) for notification purposes	No	No

Performance Data	Performance Object	ICMP	ICMP Performance Object	N / A	N / A
		IP	IP Performance Object		
		LogicalDisk	LogicalDisk Performance Object		
		Memory	Memory Performance Object		
		NBT Connection	NBT Connection Performance Object		
		Network Interface	Network Interface Performance Object		
		Network Segment	Network Segment Performance Object		
		Paging File	Paging File Performance Object		
		PhysicalDisk	PhysicalDisk Performance Object		
		Process	Process Performance Object		
		Processor	Processor Performance Object		
		System	System Performance Object		
		TCP	TCP Performance Object		
		Thread	Thread Performance Object		
		UDP	UDP Performance Object		

Reports	N / A	Daily Memory Utilization	Memory usage for the current day for Agents that have been assigned the Windows NT/2000/XP Memory Performance Data Collection Set	N / A	Yes
		Daily Process Utilization	Process usage for the current day for Agents that have been assigned the Windows NT/2000/XP Processes Performance Data Collection Set		Yes
		Daily Processor Utilization	Processor usage for the current day for Agents that have been assigned the Windows NT/2000/XP Processes Performance Data Collection Set		Yes
		Memory Utilization	Memory usage for Agents that have been assigned the Windows NT/2000/XP Memory Performance Data Collection Set		Yes

		Network - ICMP Statistics	ICMP usage for Agents that have been assigned the Windows NT/2000/XP Networking Performance Data Collection Set		Yes
		Network - IP Statistics	IP usage for Agents that have been assigned the Windows NT/2000/XP Networking Performance Data Collection Set		Yes
		Network - TCP Statistics	TCP usage for Agents that have been assigned the Windows NT/2000/XP Networking Performance Data Collection Set		Yes
		Network - UDP Statistics	UDP usage for Agents that have been assigned the Windows NT/2000/XP Networking Performance Data Collection Set		Yes
Rules	N / A	Errors	Uses Errors Filter and executes Error Beep Notification Method	N / A	Yes
		Warnings	Uses Warnings Filter and executes Warning Beep Notification Method		Yes